REQUEST FOR PROPOSALS

FOR

ACA REPORTING AND COMPLIANCE

FOR THE

PUBLIC EDUCATION EMPLOYEES' HEALTH INSURANCE PLAN

FOR

3 Year Contract Period

RFP 15-015

THIS RFP CONTAINS INFORMATION UNDER THE FOLLOWING HEADINGS:

SECTION I
General Information for the Proposer/Vendor

A. Purpose
B. Scope of Work
C. General Conditions
D. Terms of Proposal
E. Evaluation Criteria
F. Evaluation Questions
G. Security and Privacy Requirements
H. Proposal Opening
I. Key Dates
J. Delivery Schedule
K. Payment Schedule
L. Selection of Firm
M. Economy of Preparation
N. News Releases
O. Addenda to the RFP
P. Contact Point
Q. Minimum Qualifications
R. Agents

SECTION II
Information Required from Proposer/Proposers/Vendors

A. Qualifications of the Firm
B. Costs and Price Analysis

SECTION III
Criteria for Evaluation

A. General
B. Factors

SECTION IV
Additional Documents

A. State of Alabama Disclosure Statement (Required by Article 3B of Title 41, Code of Alabama 1975 – two pages)
B. Sample PEEHIP State Contract
C. Immigration Compliance Certificate
D. Proposer/Vendor Profile Form
E. Proposer/Vendor References Form
F. PEEHIP Non-Disclosure Agreement
G. Business Associate Agreement
H. PEEHIP Statement on HIPAA Compliance
I. Third Party Vendor Security Checklist
J. IRS Form W-9

SECTION I

GENERAL INFORMATION FOR THE PROPOSER/VENDOR

The Public Education Employees' Health Insurance Fund (PEEHIF) was established in 1983 under the provisions of Act 83-455 of the Alabama Legislature to provide a uniform plan of health insurance for active and retired employees of state and local educational institutions which provide instruction at any combination of grades K-14 (collectively, eligible employees), and to provide a method for funding the benefits related to the plan. The four-year universities are eligible and may elect to participate in the plan. At this time, Alabama A&M and Jacksonville State University are the only universities with active and retired members that have elected to participate in the plan. Responsibility for the establishment of the health insurance plan and its general administration and operations is vested in the Public Education Employees' Health Insurance Board (Board). The Board is a corporate body for purposes of management of the health insurance plan. All assets of the PEEHIF are held in trust for the payment of health insurance benefits. The Secretary-Treasurer of the Teachers' Retirement System of Alabama (TRS) has been statutorily appointed as the Chief Executive Officer of the PEEHIF, and also by statute, the TRS Board of Control serves as the Board of Control of the PEEHIF. In accordance with the Governmental Accounting Standards Board (GASB), the PEEHIF is considered a component unit of the State of Alabama (State) and is included in the State's Comprehensive Annual Financial Report.

The Public Education Employees' Health Insurance Plan (PEEHIP) offers a basic hospital medical plan to active members and non-Medicare eligible retirees. Benefits include inpatient hospitalization for a maximum of 365 days without a dollar limit, inpatient rehabilitation, outpatient care, physician services, and prescription drugs.

Active employees and non-Medicare eligible retirees who do not have Medicare eligible dependents can enroll in a health maintenance organization (HMO) in lieu of the basic hospital medical plan. The HMO includes hospital medical benefits, dental benefits, vision benefits, and an extensive formulary. However, participants in the HMO are required to receive care from a participating physician in the HMO plan.

The PEEHIP offers four optional plans (Hospital Indemnity, Cancer, Dental, and Vision) that may be selected in addition to or in lieu of the basic hospital medical plan or HMO. The Hospital Indemnity Plan provides a per-day benefit for hospital confinement, maternity, intensive care, cancer, and convalescent care. The Cancer Plan covers cancer disease only and benefits are provided regardless of other insurance. Coverage includes a per-day benefit for each hospital confinement related to cancer.

The Dental Plan covers diagnostic and preventative services, as well as basic and major dental services. Diagnostic and preventative services include oral examinations, teeth cleaning, x-rays, and emergency office visits. Basic and major services include fillings, general aesthetics, oral surgery not covered under a Group Medical Program, periodontics, endodontics, dentures, bridgework, and crowns. Dental services are subject to a maximum of $1,250 per year for individual coverage and $1,000 per person per year for family coverage. The Vision Plan covers annual eye examinations, eye glasses, and contact lens prescriptions.

PEEHIP members may opt to elect the PEEHIP Supplemental Plan for hospital medical coverage in lieu of the PEEHIP Hospital Medical Plan. The PEEHIP Supplemental Plan provides secondary benefits to the member's primary plan provided by another employer. Only active and non-Medicare retiree members and dependents are eligible for the PEEHIP Supplemental Plan. There is no premium required for this plan, and the plan covers most out-of-pocket expenses not covered by the primary plan. The plan cannot be used as a supplement to Medicare, the PEEHIP Hospital Medical Plan, or the State or Local Governmental Plans administered by the State Employees' Insurance Board (SEIB).

Currently there are approximately 148,000 hospital medical contracts with 312,000 covered lives.

A. PURPOSE:

REQUEST FOR PROPOSALS:

This Request For Proposals (RFP) solicits Vendor proposals for a secure software solution, preferably one that is "on-premise" to fill PEEHIP's obligation for ACA Compliance Reporting pertaining to the Affordable Care Act (ACA) Law and the Internal Revenue Code section 6055 which mandates that every provider of minimum essential coverage to individuals must report to the IRS information about the type and period of coverage and furnish the information in statements to covered individuals. In fulfilling the abovementioned obligations for ACA Compliance Reporting, the proposed solution shall include, at a minimum, ACA forms 1094-B and 1095-B as well as additional requirements that may be included in future ACA Reporting and Compliance mandates.

PEEHIP will consider a SaaS (Software as a Service) model as an alternative solution. This RFP is for a contract period of three (3) years for the Public Education Employees' Health Insurance Plan (PEEHIP) of Alabama.

B. SCOPE OF WORK

VENDOR must provide software solution as outlined below. Please indicate your agreement to each question by marking "Agree" or "Do Not Agree" for each item and include comments, as needed.

General

- Provide a software solution with fully integrated implementation including, but not limited to, training, implementation, maintenance and updates in order for PEEHIP to be ACA compliant as required by Affordable Care At (ACA) Law and the Internal Revenue Service Code section 6055, as well as additional requirements that may be included in future ACA Reporting and Compliance mandates. Proposed solution must adhere to specific filing dates as currently outlined in ACA final regulations.

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Must adhere to specific filing dates as currently outlined in the ACA final regulations

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Provide a PEEHIP network compatible software solution for on premise implementation

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Effectively support a volume of up to 200,000 contracts with 400,000 covered lives

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Allow for production of forms to be able to be stored electronically

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Provide ease of use and consistency and allow for role-based security by member name or TIN so that members can access their information on the RSA Member Online Services website

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Effectively and securely print, file, report and transmit forms 1094B and 1095B related to the Affordable Care Act (ACA) for eligible PEEHIP insured members/dependents that is in compliance with IRS AIR program as outlined in IRS publication 5165 and used in conjunction with the most current version of IRS Publications 4557, 4600, and 5164

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Implementation and configuration services

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- On site end user training

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Free of known security vulnerabilities

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Ability to systematically receive member/employee data, including indicators for deceased members, and/or members with less than 12 months of coverage, from each filer and/or by IRS form (frequency to be determined).

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Capability to receive incomplete data (blanks)

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Ability to systematically send to PEEHIP inaccurate member/employee data by filer and/or IRS form

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Secure PHI data and provide the capability to separate the data by filer

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Provide confirmation/exception reports to PEEHIP each time data is received from/sent to the filers, received from/sent to the IRS and when statements are mailed to members/employees. The confirmation/exception reports must include control totals for record counts, validate the data is accurate, complete and has not been created or destroyed

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Provide PEEHIP a pre-pass for validation of the member/employee statements and IRS filings before they are transmitted

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Please describe your ability to segregate the data by member/employee statements and IRS filings

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Ability to receive data (i.e. retro-activity, TIN changes, etc) on a monthly basis for February, March and April for the IRS filings

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Must be capable to store all information on a static basis, by filer, for auditability for a period of 10 years

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Provide timely and electronically the IRS submissions, transmittals and filings, including combined reporting (issuer/employer), mail member/employee statements, and provide systematic confirmation of filing dates for PEEHIP

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Please describe your capability, in certain situations, to use a simplified alternative method in lieu of the member/employee statements

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Ability to immediately notify filer when electronic filing errors with the IRS have occurred and require PEEHIP intervention

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Capability to respond immediately to the IRS for transmitted file issues/inaccurate data

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Ability to mask social security numbers for member/employee statements

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Ability to un-mask social security numbers for IRS filings

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Please describe your process to issue member statement corrections and update the applicable IRS form due to retro-active enrollment adjustments for member/employees in the proper time period

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Adhere to specific filing dates as outlined in the ACA final regulations

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Please describe your ability to adhere to, and remain in compliance with ACA, HIPPA, and IRS 6055/6056

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Please describe your process, to file electronic IRS ACA 30 day extensions and to communicate and document to PEEHIP the IRS approved extensions

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Please describe your capability, to respond to IRS penalty notices and provide IRS penalty abatement letters documenting reasonable cause for penalty abatement on behalf of PEEHIP

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

- Ability for authorized areas/personnel to query the system for current data and/or historical filings and reports

  _____ Agree

  _____ Do Not Agree

  Comments: _____

  _____

Technology

1. Please indicate your agreement to each question by marking “Agree” or “Do Not Agree” for each item and include comments, as needed.

2. Provide data schema to PEEHIP for uploading files to system and denote fields, via configuration, that are required during user data entry

   _____ Agree

   _____ Do Not Agree

   Comments: _____

   _____

3. Provide process for PEEHIP to make corrections to 1095-B data already populated in solution

_____ Agree

_____ Do Not Agree

Comments: _____

_____

4. Provide process for PEEHIP to delete or remove unnecessary data elements from the user interface (through configuration) as needed

_____ Agree

_____ Do Not Agree

Comments: _____

_____

5. Allow process for PEEHIP to configure the sequence and flow of the screens on the user interface

_____ Agree

_____ Do Not Agree

Comments: _____

_____

6. Allow for an internal rules engine to be configurable by PEEHIP

_____ Agree

_____ Do Not Agree

Comments: _____

_____

7. Allow for User Interface based administrative tools for:

   - Managing security and user accounts - Please list any limits to capabilities within such a role; such as, analyst, View Only, reviewer, delegator

_____ Agree

_____ Do Not Agree

Comments: _____

_____

   - Manage workflow and task routing, design screens / tabs/ user defined fields / data elements, and manage rules / validations

_____ Agree

_____ Do Not Agree

Comments: _____

_____

- Allows for the design and implementation of automatic/manual form letters and correspondence

_____ Agree

_____ Do Not Agree

Comments: _____

_____

- Provide the ability for PEEHIP to configure dropdown values for specific fields

____ Agree

_____ Do Not Agree

Comments: _____

_____

- Allow external entities to view their data only

_____ Agree

_____ Do Not Agree

Comments: _____

_____

- Allow for or support the development of a PEEHIP proprietary branch of the application

_____ Agree

_____ Do Not Agree

Comments: _____

_____

1. Describe the Technology environment / development environment that are used by the tool.

2. Describe the high level solution/technical architecture of the solution including modules that make up your solution and which ones are required and which are optional. Also describe the dependencies between modules and how changes in one module impact other modules. Provide diagrams to show data flows, workflows, message flows, and deployment. Describe the client-side processing (proprietary thick client, pure HTML, AJAX-based browser, etc.).

3. Describe the technology framework that supports your solution. This should include hardware (client and server), operating system, application server, database server, firewall, edge server, authentication server (e.g., LDAP, AD) and client software (e.g., browser) specifications as applicable to your solution.

ACA Data Collection

1. Please describe your ability to determine all invalid Tax Identification Numbers or Social Security Numbers as determined by the Social Security Administration and null Tax Identification Numbers or Social Security Numbers on both internal and external enrollment systems for initial and subsequent data clean-up.

2. Please describe your capability to create member solicitation letters and include a substitute W-9 form for members that have null or invalid data and/or provide a signed hard copy of the substitute W-9 form upon request to the IRS or Insurer.

3. Please describe your process for mailing initial and subsequent letters with substitute W-9 form and provide return postage paid envelopes to all members with null or invalid data.

4. Please describe your process to include in the solicitation various options for members to submit requested data, i.e. postage paid envelopes, dedicated phone unit to handle inbound inquiries, secure Fax number, secure email address, Member Website access.

5. Please describe your process to manage, track and store all methods of return data.

6. Please describe your process to clarify any illegible, missing or invalid data received.

7. Please describe your ability to track, store and report to Insurer all undeliverable mail.

8. Please describe your process to provide detailed reporting to Insurer and IRS providing proof of solicitation of missing or invalid data as required in accordance to “Safe Harbor” regulations.

9. Please describe your process to timely report to Insurer on all valid data collected, i.e. Tax Identification Numbers or Social Security Numbers and DOBs so Insurer’s internal and external enrollment systems can be updated.

10. Please describe your capability to perform annual data validation and solicitation of Tax Identification Numbers or Social Security Numbers based on ACA regulations.

Security

List the control reviews and certifications for data privacy and security you hold (e.g., SOC Type II, ISO, PCI DSS, etc.).

Describe how you provide information asset assurance of PEEHIP data for the following:

- In Motion (e.g., SSL/TLS, SCP, FTPS, Secure FTP, etc.)
- At Rest (e.g., encryption, segregation, anti-virus, etc.).
- In Use (e.g., Data Loss Prevention, peripheral controls, IRM / RMS, etc.)

Describe what integration services or interfaces are available for information exchange and how they are used and safeguarded (e.g., Secure File, Message Brokers, Web Services, etc.).

Describe how you provide additional safeguards for information assets requiring stricter security (e.g., Personal Health Information, Credit Card Information, etc.).

Describe your IAAA (Identity, Authentication, Authorization and Accounting) services, and what current standards are supported (e.g., SSO, access controls, SIEM, etc.) for the following:

- Internal / administrative / Remote access
- External / consumer access
- Wireless (Wi-Fi) access

- Password complexity and shared secret management
- Strong authentication
- RBAC, Context-BAC, Graded access

Provide a list of third party Proposers/Vendors / affiliates and describe the following:

- What services these entities provide
- The geographic location(s) where the services are provided
- How information is shared with the entities
- How the entities are evaluated to ensure compliance with Security standards.
- How the Print Services are audited to ensure they meet or exceed PEEHIP's standards

Describe what support exists around customer requests for vulnerability assessments, information security program review, proof of third party audit, accreditation, etc.

If PEEHIP information will be used in non-production, describe how production and non-production environments are managed, what access controls to each provide segregation of information access and any differences in the controls in-place for production versus non-production.

Implementation

Describe your implementation approach. Please provide sample implementation and integration project plans, artifacts, and staffing commitments.

Describe your approach to understanding the integration effort required for various information – vendor, financial, member/employee data, etc.

Describe the resource commitment required of PEEHIP to support the implementation.

Discuss the resource commitment for discovery, design, development / setup, configuration, import of historical contracts, training, and any additional transitional activities.

Describe your process to identify and validate requirements and ensure traceability.

Describe key challenges you have experienced with the integration of an on-demand software with enterprise solutions (i.e. PeopleSoft, SAP) and how you were able to assist your customer with the mitigation of those challenges.

What training would be normally provided to PEEHIP staff during this type of technology implementation?

As part of training support, can you provide best practice documentation to support system configurations as well as system administration guides/job aids for post go live support?

Describe the key challenges you have faced while supporting an on-demand implementation and how you mitigated those risks (understanding the vendor holds primary accountability for implementation).

Describe critical risks you have experienced around the transition of historical data and how you addressed those risks.

Describe and list the systems you currently are able to integrate with and their processes which would meet requirements as outlined.

Support

Describe your standard support levels.

Describe the proposed Account Management structure for PEEHIP.

What corrective action is taken when standards are not met? Describe your process for proactive monitoring.

How will you ensure that your program is both suited to our company's need and competitive in the market place now and in the future?

Core Competencies

Briefly describe your company's core competencies and how your company differentiates itself in the market place (e.g., specialty areas of expertise and/or value-added services).

Describe major products and/or lines of business.

State the main source of business revenue (e.g., consulting, product sales, or systems integration).

The PROPOSER/VENDOR should include high-level business flows for IRS 6055/6056 processing.

The Proposer's/Vendor's software must be completed, tested and currently processing IRS 1095 forms for clients.

The Proposer's/Vendor's software must be scalable. Describe the scalability component.

The PROPOSER/VENDOR must provide their method to protect the data in the event of a disaster. What is the r Proposer's/Vendor's recovery method?

C. GENERAL CONDITIONS

An "On-Premise" software solution model is preferred, but a SaaS, Software as a Service, model will be considered. Either solution must ensure security and confidentiality of all of organization's data.

Conflict of Interest:
The PROPOSER/VENDOR agrees that it will have no interest, direct or indirect, that will conflict in any manner or degree with the performance of services provided under a contract resulting from this RFP. The PROPOSER/VENDOR further agrees that, in the performance of the contract, the PROPOSER/VENDOR shall not employ any person having any such known interests.

Billing:
Invoices will be issued no more frequently than monthly only after services are rendered. Invoices will be paid within 30 days of receipt.

Subcontracting and Joint Ventures:
Subcontractor and Joint Ventures will not be allowed.

Termination:

Termination for Convenience: This contract may be terminated for any reason by either party with the submission of a thirty (30) day written notice thereof.

Termination for Default: PEEHIP may terminate immediately all or any part of a contract resulting from this proposal, by giving notice of default of PROPOSER/VENDOR, if the PROPOSER/VENDOR (1) refuses or fails to deliver the goods or services within the time specified, (2) fails to comply with any of the provisions of the Proposal or so fails to make progress as to endanger or hinder performance, (3) becomes insolvent or subject to proceedings under any law relating to bankruptcy, insolvency, or relief of debtors. In the event of termination for default, PEEHIP's liability will be limited to the payment for goods and/or services delivered and accepted as of the date of termination.

In the event of such termination or expiration of the agreement, PROPOSER/VENDOR shall return all accounts to PEEHIP, even those that are in repayment or have documented payment arrangements.

Failure To Execute Contract: Failure of the successful PROPOSER/VENDOR to enter into a contract in the time prescribed by PEEHIP may be cause for cancellation of the award to that PROPOSER/VENDOR. In the event the award is cancelled, the award may then be made to the second lowest responsible PROPOSER/VENDOR, or PEEHIP may reject all of the proposals.

D. TERMS OF PROPOSAL

The initial term of the Contract is anticipated to begin on November 1, 2015 and shall be for three (3) years. Contract may be renewed for two (2) optional one (1) year terms. Please indicate your agreement to each question by marking "Agree" or "Do Not Agree" for each item and include comments, as needed.

PROPOSER/VENDOR agrees that any proposal submitted will remain valid for a period of ninety (90) days from the date received by us.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

The PROPOSER/VENDOR agrees that any exceptions to the terms, conditions, or other requirements in any part of these specifications must be clearly pointed out in the appropriate section of the proposal. Otherwise, it will be considered that all items offered are in strict compliance with the specifications.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

PROPOSER/VENDOR acknowledges and agrees that PEEHIP will not under any circumstance indemnify or hold harmless PROPOSER/VENDOR, its affiliates, administrators, officers, employees or agents.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

PROPOSER/VENDOR agrees to abide by all terms and conditions set forth in the attached Sample Agreement found in Section IV-B. PROPOSER/VENDOR further agrees that any exception to those terms must be clearly set forth in the PROPOSER'S/VENDOR'S proposal; otherwise, PROPOSER/VENDOR will be deemed to have agreed to, and be bound by, each clause therein.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

PROPOSER/VENDOR agrees that PROPOSER/VENDOR shall maintain or obtain (as applicable), with respect to the activities in which PROPOSER/VENDOR engages pursuant to any Agreement that results from this RFP, professional liability (errors and omissions) insurance and general liability insurance in amounts reasonable and customary for the nature and scope of business engaged in by such party. PROPOSER/VENDOR shall deliver to PEEHIP evidence of such insurance on or before the date the Agreement goes into effect and annually thereafter. PROPOSER/VENDOR shall also name PEEHIP as an additional insured under such policies and provide documentation thereof.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

Proposals and supporting documents are kept confidential until the evaluation process is complete and a contract has been awarded. PROPOSERS/VENDORS should be aware that any information in a proposal may be subject to disclosure and/or reproduction under Alabama law once a contract has been awarded.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

Should PROPOSER/VENDOR intend to request that PEEHIP execute any document or additional terms and conditions for PEEHIP's contract that PROPOSER/VENDOR generally requires of PROPOSER/VENDOR customers, The PROPOSER/VENDOR agrees to provide a sample of such document or contract terms to PEEHIP. PROPOSER/VENDOR further agrees, however, that by accepting PROPOSER'S/VENDOR'S proposal, PEEHIP is not agreeing to and accepting the terms provided by PROPOSER/VENDOR. PEEHIP reserves the right to negotiate PROPOSER'S/VENDOR'S sample terms and conditions. In addition, PROPOSER/VENDOR acknowledges and agrees that the provision of such sample terms and conditions does not under any circumstance satisfy the requirement that the PROPOSER/VENDOR explicitly state any and all exceptions to PEEHIP's proposal specifications or Sample Agreement terms.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

VENDOR agrees to provide completed Alabama Disclosure Form, Immigration Compliance Certificate, Bidder Reference Form, Bidder Profile Form, and IRS Form W-9 with submission of proposal.

_____ Agree

_____ Do Not Agree

Comments: _____

_____

E. EVALUATON CRITERIA

PEEHIP reserves the right without qualification to select a PROPOSER/VENDOR based on, in part, but not exclusively to, the content of the proposal, experience with the PROPOSER/VENDOR, cost, and any other relevant information, including, without limitation, recommendations concerning the PROPOSER'S/VENDOR'S respective record of past performance with other clients. Each PROPOSER'S/VENDOR'S proposal will be evaluated on their:

1. Ability to provide the features listed in this RFP

2. Implementation approach

3. Price

F. EVALUATION QUESTIONS

Please answer the following questions:

a. Does PROPOSER/VENDOR have a written code of ethics, conflict of interest policy, mission statement or other related policy? If so, please provide such. Also, please complete the PROPOSER/VENDOR Profile form in Section IV Item D.

b. List at least 3 customer references for which you are providing the proposed solution (include a company's name, individual contact's name and telephone number) by completing the PROPOSER/VENDOR References Form in Section IV Item E.

c. Describe your methodology for implementing the system as described in this RFP

d. Describe the training plan. Include details about training for the core project team, system administrative users, and key PEEHIP personnel

e. Please provide the last Service Organization Controls 2 Type 2 report issued for your company

f. Please provide completed State of Alabama Disclosure Statement, Immigration Compliance Certificate (including MOU, if necessary), PROPOSER/VENDOR Profile Form, PROPOSER/VENDOR References Form, PEEHIP NDA agreement, Third Party Vendor Security Checklist and IRS Form W-9 (7 attachments)

G. SECURITY AND PRIVACY REQUIREMENTS:

PROPOSER/VENDOR will execute and maintain full compliance with the attached Business Associate Agreement (BAA) with PEEHIP found at Section IV Item G.

PROPOSER/VENDOR must also fill out the RSA Third Party Security Questionnaire found at Section IV Item H.

For the following items, please answer the questions and/or incorporate your agreement or disagreement, using the format below in your separate response document.

PROPOSER/VENDOR agrees that PEEHIP's data is PEEHIP's data, not the Proposer's/Vendor's and will be considered proprietary and will not be shared, except at PEEHIP's request, without full knowledge and express written consent.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR agrees to attach a copy of your most recently completed HIPAA assessment in the Response Documents section of the RFP. If no such assessment exists, please explain in response.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR agrees that all files in transit and at rest containing PHI must be encrypted. Examples include Secure FTP, AES 256 bit encryption, PGP, HTTPS, and hard drive encryption. Plain text emails containing PHI is strictly prohibited.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR agrees to attach copy of their Information Security Policy and Procedures in the Response Documents section of the RFP.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR agrees that if awarded the contract resulting from this RFP, they will allow PEEHIP or its agent or representative, at any point during the Agreement, to perform an on-site self-assessment based on HIPAA requirements.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR shall explain how they manage employee confidentiality/privacy barriers and compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) including the Health Information Technology for Economic and Clinical Health Act (HITECH). Detail plan(s) to ensure privacy and security of employee's information while delivering services in a worksite environment.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

All employees at PROPOSER'S/VENDOR'S organization have been trained on how to report a security incident or potential breach under HIPAA.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR must attach documents that indicate PROPOSER/VENDOR is in compliance with the PEEHIP Statement on HIPAA Compliance Document (Board Policy), Section IV Item H.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR must complete the RSA Third Party Risk Assessment found in Section IV Item I.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

PROPOSER/VENDOR must state who is responsible for ensuring compliance with all applicable laws and regulations, including but not limited to HIPAA and HITECH (Security and Privacy Officer), responsible for maintaining internal controls to protect PHI and adequate and timely steps are taken in the event of a breach of confidentiality, and responsible for communicating program and policy updates to PEEHIP and coordinating as necessary with PEEHIP's internal counsel and staff. At a minimum, please include:

a. The total number of dedicated staffing

b. Include in your hierarchy whether there is a defined security and privacy office, and list their background and experience that supports their qualifications for this role.

(a) ____ Agree (b) ____ Disagree (c) ____ Comment

_____

Has PROPOSER/VENDOR ever had a HIPAA breach? If so, please provide explanation including correction/revision of processes and procedures, mitigation of effect of breach and any remuneration made.

_____Confirmed _____ Not Confirmed

Comments_____

Please confirm all employees at your organization have been trained on how to report a security incident or potential breach.

_____Confirmed _____ Not Confirmed

Comments_____

Please explain how PROPOSER/VENDOR complies with HIPAA's workforce clearance procedures. Are all employees background checked and how often.

Please confirm if any of PROPOSER'S/VENDOR'S staff are based outside of the US? If yes, please provide the details of their credentials.

_____Confirmed _____ Not Confirmed

Comments_____

Please provide details of how seamless operations are achieved and quality controls are in place for off-shore operations.

H. PROPOSAL OPENING:

All proposals will be submitted (six (6) copies) in a sealed wrapper with the following plainly marked on the front:

RETIREMENT SYSTEMS OF ALABAMA
PEEHIP ACA COMPLIANCE SOFTWARE
RFP 15-015
OPENING September 15, 2015
Proposals will be sent to:

Via UPS or FedEx:

Mr. Edward Davis
Director of Office Services
Retirement Systems of Alabama
201 South Union Street
Montgomery, AL 36104

Via US Mail

Mr. Edward Davis
Director of Office Services
Retirement Systems of Alabama
P.O. Box 302150
Montgomery, AL 36130-2150

Proposals may be hand delivered to Room 574 of the Retirement Systems Building, 201 South Union Street, Montgomery, Alabama. **Proposals will be accepted until 2:00 p.m. CT on September 15, 2015,** and opened at that time. Proposals will not be accepted after this date and time. The PEEHIP reserves the right to reject any and all responses to this RFP.

Any questions regarding this RFP must be submitted electronically via email by September 8, 2015, at 2:00 p.m. CT to Mr. Edward Davis at Edward.Davis@rsa-al.gov.

I. KEY DATES:

RFP 15-015 Key Dates:

Activity	Date
RFP issued	August 27, 2015
Deadline to submit questions	September 8, 2015
Responses to questions posted to PEEHIP website	September 11, 2015
Bid responses due by	September 15, 2015
Bid opening date	September 15, 2015
Finalist conferences with solution demonstration	September 24 – 25, 2015
Award of bid	September 30, 2015

J. DELIVERY SCHEDULE:

PEEHIP desires to begin implementing this software from awarded PROPOSER/VENDOR within ten (10) days of signed contract with PROPOSER/VENDOR and that PROPOSER/VENDOR shall be prepared to provide all abovementioned products and training to PEEHIP no later than October 15, 2015.

K. PAYMENT SCHEDULE:

Payment will be made within 30 days of invoice upon receipt of product/services.

L. SELECTION OF FIRM:

PEEHIP expects to contract with the successful PROPOSER/VENDOR. All responding PROPOSERS/VENDORS will be notified in writing within a reasonable length of time following the selection. Prior to the selection of a firm, two or more PROPOSERS/VENDORS shall be requested to make oral presentations and software demonstration via phone/webex to the evaluation committee. The proposal shall become the property of the PEEHIP.

M. ECONOMY OF PREPARATION:

Proposals should be prepared simply and economically and provide a concise description of the PROPOSER'S/VENDOR'S response to the requirements of this RFP. Emphasis should be on clarity. The PEEHIP will not be responsible for any costs incurred by any PROPOSER/VENDOR in the preparation of a proposal.

N. NEWS RELEASES:

News releases pertaining to this RFP, the service, or the audits to which it relates will be made only with prior written approval of the CEO or his representative.

O. ADDENDA TO THE RFP:

Any modifications made to the RFP prior to the proposal due date will be provided in writing to all solicited Proposers/Vendors.

P. CONTACT POINT:

Any questions that arise concerning this RFP may be directed to Ed Davis at Edward.Davis@rsa-al.gov

Q. MINIMUM QUALIFICATIONS:

To be considered a viable proposer, the following minimum requirements must be met. Please indicate your agreement to each item by marking "Agree" or "Do Not Agree" for each item and include comments, as needed. If there are any requirements below that PROPOSER/VENDOR does not meet, please mark Does Not Apply.

- PROPOSER/VENDOR must not have any bankruptcy filings within last five (5) years

- PROPOSER/VENDOR must have experience with at least ten (10) clients successfully utilizing proposed solution for ACA Compliance and Reporting

- PROPOSER'S/VENDOR'S senior officers, board members, or directors must not have any felony convictions

- PROPOSER/VENDOR must have experience with at least ten (10) clients successfully utilizing proposed solution for ACA Compliance and Reporting

- PROPOSER/VENDOR must be HIPAA compliant

__ Agree

__ Do Not Agree

Comments: _____

_____

R. AGENTS:

No agents fees will be payable by PEEHIP or successful PROPOSER/VENDOR. PEEHIP will respond only to parties interested in proposing and performing the services.

SECTION II

INFORMATION REQUIRED FROM PROPOSER/PROPOSERS/VENDORS

Proposals must be submitted in the format outlined below:

A. QUALIFICATIONS OF THE FIRM:

1. BUSINESS ORGANIZATION

   State the full name and address of your organization, and if applicable, the branch office or other subordinate element that will perform or assist in performing the work hereunder. Indicate whether you operate as an individual, partnership, or corporation; if as a corporation, include the state in which you incorporated. State whether you are licensed to operate in the State of Alabama.

2. PRIOR EXPERIENCE:

   As part of your proposal, include a brief statement (maximum five pages) concerning the relevant experience of persons from your firm who will be implementing the services for the proposed solution for PEEHIP. Do not include general corporate background brochures.

3. MANPOWER:

   Identify lead individuals by name and title and include a resume of each.

4. AUTHORIZED OFFICIALS:

   Include the names and telephone numbers of personnel of the organization authorized to execute the proposed contracts with the PEEHIP.

5. ADDITIONAL INFORMATION AND COMMENTS:

   Include any other information believed to be pertinent but not specifically requested elsewhere in this RFP.

B. COST AND PRICE ANALYSIS:

The information requested in this Section is required to support the reasonableness of your proposal price. Use the following format:

Reflect the details of each of the following you expect for the services for each of three (3) contract years.

- Itemized estimated cost for the proposed solution
- Itemize other direct cost that may be included in billing for these services and basis for billing
- Expected total contract cost by year for each of the three (3) years

NOTE: PEEHIP will not be liable for any expense that is not identified in the Proposer's/Vendor's response.

PEEHIP desires to enter into a three (3) year contract for the specified services.

SECTION III

CRITERIA FOR EVALUATION

A. GENERAL:

Proposals will be evaluated by an evaluation committee. Selection will be based on all factors listed below and others implicit within the RFP and will represent the best performance and reasonable costs for the PEEHIP. Oral presentations and interviews (in person) may be required as part of the evaluation criteria.

B. FACTORS:

The following factors will be the minimum criteria in making the selection (order does not indicate priority):

1. PRICE*:*
   This criterion shall be judged by its reasonableness in relation to the merits of the proposal.

2. QUALIFICATION OF THE FIRM*:*
   This includes the ability of the PROPOSER/VENDOR to meet the terms of the RFP.

3. ACCOUNT PERSONNEL:
   The competence and level of professional personnel who will perform the services will be considered.

SECTION IV

ADDITIONAL DOCUMENTS

The following documents are referenced in this RFP and must be completed and submitted with the proposal:

A. State of Alabama Disclosure Statement (Required by Article 3B of Title 41, Code of Alabama 1975) – two pages

B. Sample PEEHIP State Contract

C. Immigration Compliance Certificate

D. Proposer/Vendor Profile Form

E. Proposer/Vendor References Form

F. PEEHIP Non-Disclosure Agreement

G. Business Associate Agreement

H. PEEHIP Statement on HIPAA Compliance

I. Third Party Vendor Security Checklist

J. IRS Form W-9

State of Alabama

Disclosure Statement

(Required by Act 2001-955)

ENTITY COMPLETING FORM

ADDRESS

CITY, STATE, ZIP TELEPHONE NUMBER ( )

STATE AGENCY/DEPARTMENT THAT WILL RECEIVE GOODS, SERVICES, OR IS RESPONSIBLE FOR GRANT AWARD

ADDRESS

CITY, STATE, ZIP TELEPHONE NUMBER ( )

This form is provided with:

Contract Proposal Request for Proposal Invitation to Bid Grant Proposal

Have you or any of your partners, divisions, or any related business units previously performed work or provided goods to any State Agency/Department in the current or last fiscal year?

Yes No

If yes, identify below the State Agency/Department that received the goods or services, the type(s) of goods or services previously provided, and the amount received for the provision of such goods or services.

STATE AGENCY/DEPARTMENT	TYPE OF GOODS/SERVICES	AMOUNT RECEIVED

Have you or any of your partners, divisions, or any related business units previously applied and received any grants from any State Agency/Department in the current or last fiscal year?

Yes No

If yes, identify the State Agency/Department that awarded the grant, the date such grant was awarded, and the amount of the grant.

STATE AGENCY/DEPARTMENT	DATE GRANT AWARDED	AMOUNT OF GRANT

1. List below the name(s) and address(es) of all public officials/public employees with whom you, members of your immediate family, or any of your employees have a family relationship and who may directly personally benefit financially from the proposed transaction. Identify the State Department/Agency for which the public officials/public employees work. (Attach additional sheets if necessary.)

NAME OF PUBLIC OFFICIAL/EMPLOYEE	ADDRESS	STATE DEPARTMENT/AGENCY

2. List below the name(s) and address(es) of all family members of public officials/public employees with whom you, members of your immediate family, or any of your employees have a family relationship and who may directly personally benefit financially from the proposed transaction. Identify the public officials/public employees and State Department/Agency for which the public officials/public employees work. (Attach additional sheets if necessary.)

NAME OF FAMILY MEMBER	ADDRESS	NAME OF PUBLIC OFFICIAL/ PUBLIC EMPLOYEE	STATE DEPARTMENT/ AGENCY WHERE EMPLOYED

If you identified individuals in items one and/or two above, describe in detail below the direct financial benefit to be gained by the public officials, public employees, and/or their family members as the result of the contract, proposal, request for proposal, invitation to bid, or grant proposal. (Attach additional sheets if necessary.)

Describe in detail below any indirect financial benefits to be gained by any public official, public employee, and/or family members of the public official or public employee as the result of the contract, proposal, request for proposal, invitation to bid, or grant proposal. (Attach additional sheets if necessary.)

List below the name(s) and address(es) of all paid consultants and/or lobbyists utilized to obtain the contract, proposal, request for proposal, invitation to bid, or grant proposal:

NAME OF PAID CONSULTANT/LOBBYIST	ADDRESS

By signing below, I certify under oath and penalty of perjury that all statements on or attached to this form are true and correct to the best of my knowledge. I further understand that a civil penalty of ten percent (10%) of the amount of the transaction, not to exceed $10,000.00, is applied for knowingly providing incorrect or misleading information.

Signature Date

Notary's Signature Date Date Notary Expires

Act 2001-955 requires the disclosure statement to be completed and filed with all proposals, bids, contracts, or grant proposals to The State of Alabama in excess of $5,000.

STATE OF ALABAMA
MONTGOMERY COUNTY

AGREEMENT

This Agreement, which results from RFP _____ entitled _____, is made and entered into effective _____ between the Public Education Employees' Health Insurance Plan and _____, hereinafter referred to as "Contractor."

SERVICES

Contractor shall provide Secure Software Solution to PEEHIP in accordance with the guidelines, terms and conditions set forth in PEEHIP's RFP _____ and Contractor's Proposal dated _____, all of which documents are attached hereto as Exhibit A and incorporated herein by reference.

CONSIDERATION

As consideration for the services rendered pursuant to the Agreement, PEEHIP agrees to compensate the Contractor an amount equal to the rates set forth in Contractor's Proposal, as amended by the Contractor's Revised Proposal.

TERM

This Agreement shall be for the period beginning _____ and ending _____.

OTHER

Contractor acknowledges and understands that this Agreement is not effective until it has received all required state government approvals, and Contractor shall not begin performing work under this Agreement until notified to do so by PEEHIP. Contractor is entitled to no compensation for work performed prior to the effective date of this Agreement.

Contractor acknowledges that Contractor is an independent contractor, and neither Contractor nor Contractor's employees are to be considered employees of PEEHIP or entitled to benefits under the State of Alabama Merit System.

In the event of proration of the funds from which this Agreement is to be paid, the Agreement will be subject to termination by PEEHIP.

Contractor acknowledges that the terms and commitments contained herein shall not be constituted as a debt of the State of Alabama in violation of Article 11, Section 213 of the Constitution of Alabama, 1901, as amended by Amendment Number 26. It is further agreed that if any provisions of this Agreement shall contravene any statute or Constitutional provision or amendment, either now in effect or which may, during the course of this Agreement, be enacted, then that conflicting provision in the Agreement shall be deemed null and void. Contractor may not assign this Agreement or any interest herein or any money due hereunder without the expressed written consent of PEEHIP. Contractor's sole remedy for the settlement of any and all disputes arising under the terms of this Agreement shall be limited to the filing of a claim with the Board of Adjustment of the State of Alabama.

To the fullest extent permitted by law, Contractor shall indemnify, defend, and hold harmless PEEHIP, the State of Alabama, the Retirement Systems of Alabama, and their affiliates, and their respective administrators, officers, directors, agents, and employees (the "Indemnitees"), from and against any and all claims, damages, losses, and expenses, including but not limited to reasonable attorney's fees, arising out of or resulting from Contractor's performance of Services under this Agreement and/or any other of Contractor's acts and/or omissions under this Agreement. Without limiting the foregoing in any manner, Contractor shall indemnify, defend and hold harmless the Indemnitees from and against any and all claims, damages, losses and expenses, including but not limited to reasonable attorney's fees, (a) incurred as a result of Contractor's (or Contractor's agent's) violation of any law, rule or regulation; (b) arising out of, or related to, Contractor's (or Contractor's agent's) breach of warranty or representation; or (c) arising out of, or related to, Contractor's (or Contractor's agent's) negligent or willful misconduct. For all claims against the Indemnitees by any employee, agent, or any other person directly or indirectly employed by Contractor, the indemnification obligation under this paragraph shall not be limited in any way by any limitation on the amount or type of damages, compensation or benefits payable by or for Contractor or its agents, under worker's compensation laws, disability benefits laws or other employee benefits laws.

Contractor acknowledges and agrees that, notwithstanding anything to the contrary contained herein or in any other Agreement between the parties hereto, PEEHIP shall not indemnify or hold harmless Contractor, its affiliates, administrators, officers, employees or agents. Contractor further acknowledges and agrees that PEEHIP shall not be liable to Contractor for any late fees, penalties, collection fees or attorney fees unless specifically agreed to in a writing signed by PEEHIP.

Contractor agrees that Contractor shall maintain or obtain (as applicable), with respect to the activities in which Contractor engages pursuant to any Agreement that results from this RFP, professional liability (errors and omissions) insurance and general liability insurance in amounts reasonable and customary for the nature and scope of business engaged in by such party. Contractor shall deliver to PEEHIP evidence of such insurance on or before the date the Agreement goes into effect and annually thereafter. Contractor shall also name PEEHIP as an additional insured under such policies and provide documentation

Contractor acknowledges that, in the course of performing its responsibilities under this Agreement, Contractor may be exposed to or acquire information that is proprietary or confidential to PEEHIP or its members. Contractor agrees to hold such information in confidence and not to copy, reproduce, sell, assign, license, market, transfer or otherwise disclose such information to third parties or to use such information for any purpose whatsoever, without the express written permission of PEEHIP, other than for the performance of obligations hereunder or as required by applicable state or federal law. For purposes of this Agreement, all records, financial information, specifications and data disclosed to Contractor during the term of this Agreement, whether submitted orally, in writing, or by any other media, shall be deemed to be confidential in nature unless otherwise specifically stated in writing by PEEHIP.

Contractor acknowledges that all data relating to PEEHIP or PEEHIP's beneficiaries is owned by PEEHIP and constitutes valuable property of PEEHIP. PEEHIP shall retain ownership of, and all other rights and interests with respect to, its data (including, without limitation, the content thereof, and any and all copies, modifications, alterations, and enhancements thereto, and any derivative works resulting therefrom), and nothing herein shall be construed as granting Contractor any ownership, license or any other rights of any nature with respect thereto. Contractor may not use PEEHIP's data (including de-identified data) for any purpose other than providing the Services contemplated hereunder. Upon termination of the Agreement, Contractor agrees to return or destroy all copies of PEEHIP data in its possession or control except to the extent such data must be retained pursuant to applicable law.

By signing this contract, the contracting parties affirm, for the duration of the Agreement, that they will not violate federal immigration law or knowingly employ, hire for employment, or continue to employ an unauthorized alien within the state of Alabama. Furthermore, a contracting party found to be in violation of this provision shall be deemed in breach of the agreement and shall be responsible for all damages resulting therefrom.

Contractor acknowledges that PEEHIP may be subject to Alabama open records laws or similar state and/or federal laws relating to disclosure of public records and may be required, upon request, to disclose certain records and information covered by and not exempted from such laws. Contractor acknowledges and agrees that PEEHIP may comply with those laws without violating any provision of Contractor's proposal or this final Agreement. Contractor agrees to intervene in and defend any lawsuit brought against PEEHIP, the Retirement Systems of Alabama, or any of their respective employees, agent or directors, for their refusal to provide Contractor's alleged confidential and/or proprietary information to a requesting party. PEEHIP shall provide Contractor written notice of any such lawsuit within ten (10) days of receipt of service by PEEHIP. Contractor shall intervene within thirty (30) days of notice or will be deemed to have waived any and all

claim that the information is confidential and/or proprietary and any and all claims against PEEHIP for disclosure of Contractor's alleged confidential and/or proprietary information.

APPLICABLE LAW

This Agreement shall be governed by and construed in accordance with Alabama Law, without giving any effect to the conflict of laws provision thereof.

TERMINATION

Termination for Convenience: This contract may be terminated for any reason by either party with the submission of a thirty (30) day written notice thereof.

Termination for Default: PEEHIP may terminate immediately all or any part of a contract resulting from this proposal, by giving notice of default of PROPOSER/VENDOR, if the PROPOSER/VENDOR (1) refuses or fails to deliver the goods or services within the time specified, (2) fails to comply with any of the provisions of the Proposal or so fails to make progress as to endanger or hinder performance, (3) becomes insolvent or subject to proceedings under any law relating to bankruptcy, insolvency, or relief of debtors. In the event of termination for default, PEEHIP's liability will be limited to the payment for goods and/or services delivered and accepted as of the date of termination.

In the event of such termination or expiration of the agreement, PROPOSER/VENDOR shall return all accounts to PEEHIP, even those that are in repayment or have documented payment arrangements.

Failure To Execute Contract: Failure of the successful PROPOSER/VENDOR to enter into a contract in the time prescribed by PEEHIP may be cause for cancellation of the award to that PROPOSER/VENDOR. In the event the award is cancelled, the award may then be made to the second lowest responsible PROPOSER/VENDOR, or PEEHIP may reject all of the proposals.

[SIGNATURE PAGE TO FOLLOW]

Contractor Federal Tax ID Number

By: _____

Its: _____

Public Education Employees' Health Insurance Plan

By: David G. Bronner
Its: Chief Executive Officer

Legally reviewed and approved by:

Legal Counsel for PEEHIP

AND

Approved by:

_____
Governor Robert Bentley
State of Alabama

State of _____

County of _____

CERTIFICATE OF COMPLIANCE WITH THE BEASON-HAMMON ALABAMA TAXPAYER AND CITIZEN PROTECTION ACT

(ACT 2011-535, as amended by ACT 2012-491)

DATE: _____

RE: Contract/Grant/Incentive (*describe by number or subject):* _____by and between _____(Contractor/Grantee) and _____State Agency, Department of Public Entity)

The undersigned herby certifies to the State of Alabama as follows:

1. The undersigned holds the position of _____with the Contractor/Grantee named above, and is authorized to provide representations set out in this Certificate as the official and binding act of that entity, and has knowledge of the provisions of **THE BEASON-HAMMON ALABAMA TAXPAYER AND CITIZEN PROTECTION ACT** (ACT 2011-535 of the Alabama Legislature, as amended by Act 2012-491) which is described herein as "the Act".
2. Using the following definitions from Section 3 of the Act, select and initial either (a) or (b), below, to describe the Contractor/Grantee's business structure.

> **BUSINESS ENTITY**: Any person or group of persons employing one or more persons performing or engaging in any activity, enterprise, profession, or occupation for gain, benefit, advantage, or livelihood, whether for profit or not for profit. "Business entity" shall include, but not be limited to the following:
>
> a. Self-employed individuals, business entities filing articles of incorporation, partnerships, limited partnerships, limited liability companies, foreign corporations, foreign limited partnerships, foreign limited liability companies authorized to transact business in this state, business trusts, and any business entity that registers with the Secretary of State.
>
> b. Any business entity that possesses a business license, permit, certificate, approval, registration, charter, or similar form of authorization issued by the state, any business entity that is exempt by law from obtaining such a business license and any business entity that is operating unlawfully without a business license.
>
> **EMPLOYER:** Any person, firm, corporation, partnership, joint stock association, agent, manager, representative, foreman, or other person having control or custody of any employment, place of employment, or of any employee, including any person or entity employing any person for hire within the State of Alabama, including a public employer. This term shall not include the occupant of a household contracting with another person to perform casual domestic labor within the household.

____(a) the Contractor/grantee is a business entity or employer as those terms are defined in Section 3 of the Act. The Contractor/Grantee must attach a copy of its complete *E-Verify Memorandum of Understanding* issued and electronically signed by the U.S. Department of Homeland Security when the business entity or employer enrolls in the E-Verify program to this Certificate of Compliance.

___(b) The Contractor/Grantee is not a business entity or employer as those terms are defined in Section 3 of the Act.

3. As of the date of this Certificate, Contractor/Grantee does not knowingly employ an unauthorized alien within the State of Alabama and hereafter it will not knowingly employ, hire for employment, or continue to employ an unauthorized alien within the State of Alabama;
4. Contractor/Grantee is enrolled in E-verify unless it is not eligible to enroll because of the rules of that program or other factor beyond its control.

Certified this_____day of _____20 ___.

_____
Name of Contractor/Grantee/Recipient
By:

_____
Its:

The above Certification was signed in my presence by the person whose name appears above, on

This_____day of _____20_____.

WITNESS_____

_____
Printed Name of Witness

Proposer/Vendor
Profile Form

Proposer/Vendor's Legal Name:	Address:	
Phone Number:	Fax Number:	E-mail:
Home Office Location:	Date Established:	Ownership: If corporation, State in which you are Incorporated :
Firm Leadership:	Number of Employees:	Number of Employees Directly Involved in Tasks Related to the Work:
Is your firm licensed to operate in the State of Alabama?		
Additional Background Information:		

Proposer/Vendor
References Form

Three professional references who have received services from the Proposer/Vendor in the past three years:

Company Name:	Contact Name:
Address:	Phone Number: E-mail:
Project Name:	Beginning Date of Project: Ending Date of Project:
Description of project size, complexity and role in this project.	
Company Name:	Contact Name:
Address:	Phone Number: E-mail:
Project Name:	Beginning Date of Project: Ending Date of Project:
Description of project size, complexity and role in this project.	
Company Name:	Contact Name:
Address:	Phone Number: E-mail:
Project Name:	Beginning Date of Project: Ending Date of
Description of project size, complexity and role in this project.	

Alabama Public Education Employees' Health Insurance Plan (PEEHIP)
Confidentiality and Non-Disclosure Agreement

This Agreement is entered into this ___ day of _____, 20__ by and between _____ with offices at _____ (hereinafter "Recipient") and the Alabama Public Education Employees Health Insurance Plan, headquartered in Montgomery, Alabama (hereinafter "PEEHIP").

WHEREAS PEEHIP possesses information that is confidential and proprietary to PEEHIP (hereinafter "Confidential Information"); and

WHEREAS the Recipient is willing to receive disclosure of the Confidential Information pursuant to the terms of this Agreement for the purpose of _____.

NOW THEREFORE, in consideration for the mutual undertakings of PEEHIP and the Recipient under this Agreement, the parties agree as follows:

1. Disclosure. PEEHIP agrees to disclose, and Recipient agrees to receive the Confidential Information.

2. Confidentiality.

2.1 No Use. Recipient agrees not to use the Confidential Information in any way except for the purpose set forth above.

2.2. No Disclosure. Recipient agrees to use its best efforts to prevent and protect the Confidential Information, or any part thereof, from disclosure except for the purpose set forth above and as permitted by the HIPAA Privacy Rule.

2.3 Protection of Secrecy. Recipient agrees to take all steps reasonably necessary to protect the secrecy of the Confidential Information, and to prevent the Confidential Information from falling into the public domain or into the possession of unauthorized persons.

3. Limits on Confidential Information. Confidential Information shall not be deemed proprietary and the Recipient shall have no obligation with respect to such information where the information:

(a) was known to Recipient prior to receiving any of the Confidential Information from PEEHIP;

(b) has become publicly known through no wrongful act of Recipient;

(c) was received by Recipient without breach of this Agreement from a third party without restriction as to the use and disclosure of the information;

(d) was independently developed by Recipient without use of the Confidential Information; or

(e) was ordered to be publicly released by the requirement of a government agency.

4. Ownership of Confidential Information. Recipient agrees that all Confidential Information shall remain the property of PEEHIP, and that PEEHIP may use such Confidential Information for any

purpose without obligation to Recipient. Nothing contained herein shall be construed as granting or implying any transfer of rights to Recipient in the Confidential Information, or any patents or other intellectual property protecting or relating to the Confidential Information.

5. Term and Termination. The obligations of this Agreement shall be continuing until the Confidential Information disclosed to Recipient is no longer confidential. This agreement shall continue in the event the above stated purpose service agreement is ended for any reason.

6. Survival of Rights and Obligations. This Agreement shall be binding upon, inure to the benefit of, and be enforceable by (a) PEEHIP, its successors, and assigns; and (b) Recipient, its successors and assigns.

IN WITNESS WHEREOF, the parties have executed this agreement effective as of the date first written above.

PEEHIP	RECIPIENT (_____)
Signed:	Signed:
_____	_____
Print Name:	Print Name:
_____	_____
Title:	Title:
_____	_____
Date:	Date:
_____	_____

BUSINESS ASSOCIATE AGREEMENT

This Agreement is made and entered into this _____ day of _____, 2014, by and between _____ ("Business Associate") and the Public Education Employees' Health Insurance Board ("Plan Sponsor"), acting on behalf of the Public Education Employees' Health Insurance Plan ("Covered Entity").

WHEREAS, Business Associate and Covered Entity desire and are committed to complying with all relevant federal and state laws with respect to the confidentiality and security of Protected Health Information (PHI), including, but not limited to, the federal Health Insurance Portability and Accountability Act of 1996, and accompanying regulations, as amended from time to time (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH), and any regulations promulgated thereunder.

NOW, THEREFORE, for valuable consideration the receipt of which is hereby acknowledged and intending to establish a business associate relationship under 45 CFR §164, the parties hereby agree as follows:

I. Definitions

A. "Business Associate" shall have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Advanced Pharmacy Concepts, Inc.

B. "Breach" shall be defined as set out in 45 CFR §164.402.

C. "CFR" means the Code of Federal Regulations. A reference to a CFR section means that section as amended from time to time; provided that if future amendments change the designation of a section referred to herein, or transfer a substantive regulatory provision referred to herein to a different section, the section references herein shall be deemed to be amended accordingly.

D. "Compliance Date(s)" shall mean the date(s) established by the Secretary or the United States Congress as the effective date(s) of applicability and enforceability of the Privacy Rule, Security Rule and HITECH Standards.

E. "Designated Record Set" shall have the same meaning as the term "designated record set" in 45 CFR §164.501 and shall include a group of records that is: (i) the enrollment, payment, claims adjudication and case or medical management record systems maintained by or for Covered Entity by Business Associate or (2) used, in whole or in part, by or for Covered Entity to make decisions about Individuals.

F. "Electronic Protected Health Information" (EPHI) shall have the same meaning as the term "electronic protected health information" in 45 CFR §160.103, limited to the information received from or created on behalf of Covered Entity by Business Associate.

G. "HITECH Standards" shall mean the privacy, security and security breach notification provisions applicable to a Business Associate under Subtitle D of the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009, as such law may be amended from time to time, and any regulations promulgated thereunder.

H. "Individual" shall have the same meaning as the term "individual" in 45 CFR §160.103, and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).

I. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and E.

J. "Protected Health Information" (PHI) shall have the same meaning as the term "protected health information" in 45 CFR §160.103, limited to the information received from or created on behalf of Covered Entity by Business Associate.

K. "Required by Law" shall have the same meaning as the term "required by law" in 45 CFR §164.501.

L. "Security Incident" shall have the same meanings as the term "security incident" in 45 CFR §164.304.

M. "Security Rule" shall mean the Standards for the Protection of Electronic Protected Health Information at 45 CFR parts 160 and 164, subparts A and C.

N. "Unsecured PHI" shall have the same meaning as "unsecured protected health information" in 45 CFR §164.402.

Terms used, but not otherwise defined, shall have the same meaning as those terms in the Privacy Rule, Security Rule and HITECH Standards.

II. Obligations of Business Associate

A. Business Associate agrees not to use or disclose PHI other than as permitted or required by this Agreement or as Required by Law. Business Associate will take reasonable efforts to limit requests for, use and disclosure of PHI to the minimum necessary to accomplish the intended request, use or disclosure and comply with 45 CFR 164.502(b) and 514(d) .

B. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate shall implement administrative, physical, and technical safeguards (including written policies and procedures) that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI that it creates, receives, maintains, or transmits on behalf of the Covered Entity as required by the Security Rule.

C. Business Associate agrees to report to Covered Entity any use or disclosure of PHI other than as provided for by this Agreement promptly after Business Associate has actual knowledge of such use or disclosure, and to report promptly to the Covered Entity all Security Incidents of which it becomes aware. Following the discovery of a Breach of Unsecured PHI, Business Associate shall notify Covered Entity of such Breach without unreasonable delay, and in no event later than 30 calendar days after such discovery. The notification will include the identification of each individual whose Unsecured PHI has been, or is reasonably believed to have been, accessed, acquired or disclosed during the Breach. A Breach shall be treated as discovered as of the first day on which such Breach is known or reasonably should have been known to Business Associate. The parties acknowledge and agree that this section constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity is required by applicable laws or regulations. "Unsuccessful Security Incidents" shall include, but not be limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI, and so long as additional notice to Covered Entity is not required by applicable laws or regulations.

D. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this Agreement or applicable regulations. Business Associate has a duty to assist the Covered Entity in any mitigation, notice, reporting, or other remedial actions required, all of which would be at the Covered Entity's request and in the Covered Entity's sole discretion.

E. Business Associate agrees to include in its agreement with any agent or subcontractor to whom it provides PHI on behalf of the Covered Entity conditions with respect to such information that are at least as restrictive as those that apply through this Agreement to Business Associate. Business Associate agrees to ensure that any agents, including sub-agents, to whom it provides EPHI received from, or created or received by Business Associate on behalf of the Covered Entity, agree in writing to implement the same reasonable and appropriate safeguards that apply to Business Associate to protect the Covered Entity's EPHI.

F. If Business Associate maintains PHI in a Designated Record Set, Business Associate agrees to make available to Covered Entity, within a reasonable time, such information as Covered Entity may require to fulfill Covered Entity's obligations to respond to a request for access to PHI as provided under 45 CFR §164.524 or to respond to a request to amend PHI as required under 45 CFR §164.526. Business Associate shall refer to Covered Entity all such requests that Business Associate may receive from Individuals. If Covered Entity requests Business Associate to amend PHI in Business Associate's possession in order to comply with 45 CFR §164.526, Business Associate shall effectuate such amendments no later than the date they are required to be made by 45 CFR §164.526; provided that if Business Associate receives such a request from Covered Entity less than ten (10) business days prior to such date, Business Associate will effectuate such amendments as soon as is reasonably practicable.

G. If applicable, Business Associate agrees to provide to Covered Entity within a reasonable time such information necessary to permit Covered Entity to respond to a request by an Individual for an accounting of disclosures as provided under 45 CFR §164.528. Business Associate shall refer to Covered Entity all such requests which Business Associate may receive from Individuals.

H. Upon reasonable notice, Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to the U.S. Secretary of Health and Human Services, or an officer or employee of that Department to whom relevant authority has been delegated, at Covered Entity's expense in a reasonable time and manner, for purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule.

I. Notwithstanding any other provision in this Agreement, Business Associate hereby acknowledges and agrees that to the extent it is functioning as a Business Associate of Covered Entity, Business Associate will comply with the HITECH Business Associate provisions and with the obligations of a Business Associate as prescribed by HIPAA and the HITECH Act commencing on the Compliance Date of each such provision. Business Associate and the Covered Entity further agree that the provisions of HIPAA and the HITECH Act that apply to Business Associates and that are required to be incorporated by reference in a Business Associate Agreement are incorporated into this Agreement between Business Associate and Covered Entity as if set forth in this Agreement in their entirety and are effective as of the Compliance Date.

III. Permitted Uses and Disclosures by Business Associate

Except as otherwise limited in this Agreement, Business Associate may:

A. Use or disclose Protected Health Information on behalf of the Covered Entity, if such use or disclosure of Protected Health Information would not violate the Privacy Rule, including the minimum necessary standard, if done by the Covered Entity.

B. Use or disclose PHI to perform the services outlined in this RFP.

C. Use Protected Health Information for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate.

D. Disclose Protected Health Information for the proper management and administration of Business Associate or to fulfill any present or future legal responsibilities of Business Associate, provided that such disclosure is either Required by Law or Business Associate obtains reasonable assurances from any person to whom Protected Health Information is disclosed that such person will: (i) keep such information confidential, (ii) use or further disclose such information only for the purpose for which it was disclosed to such person or as Required by Law, and (iii) notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

E. Use Protected Health Information to provide data aggregation services relating to the health care operations of the Covered Entity, as provided in 45 CFR §164.501.

F. To create de-identified data, provided that the Business Associate de-identifies the information in accordance with the Privacy Rule. De-identified information does not constitute PHI and is not subject to the terms and conditions of this Agreement.

G. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

H. Business Associate agrees to ensure that access to EPHI related to the Covered entity is limited to those workforce members who require such access because of their role or function. Business Associate agrees to implement safeguards to prevent its workforce members who are not authorized to have access to such EPHI from obtaining access and to otherwise ensure compliance by its workforce with the Security Rule

IV. Obligations of Covered Entity

A. Covered Entity shall notify Business Associate of any facts or circumstances that affect Business Associate's use or disclosure of PHI. Such facts and circumstances include, but are not limited to: (i) any limitation or change in Covered Entity's notice of privacy practices, (ii) any changes in, or withdrawal of, an authorization provided to Covered Entity by an Individual pursuant to 45 CFR §164.508; and (iii) any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 CFR §164.522.

B. Covered Entity warrants that it will not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule or is not otherwise authorized or permitted under this Agreement.

C. Covered Entity acknowledges and agrees that the Privacy Rules allow the Covered Entity to permit Business Associate to disclose or provide access to PHI, other than Summary Health Information, to the Plan Sponsor only after the Plan Sponsor has amended its plan documents to provide for the permitted and required uses and disclosures of PHI and to require the Plan Sponsor to provide a certification to the Plan that certain required provisions have been incorporated into the Plan documents before the Plan may disclose, either directly or through a Business Associate, any PHI to the Plan Sponsor. Covered Entity hereby warrants and represents that Plan documents have been so amended and that the Plan has received such certification from the Plan Sponsor.

D. Covered Entity agrees that it will have entered into Business Associate Agreements with any third parties to whom Covered Entity directs and authorizes Business Associate to disclose PHI.

V. Effective Date; Termination

A. The effective date of this Agreement shall be the date this Agreement is signed by both parties (or the Compliance Date, if later).

B. This Agreement shall terminate on the date Business Associates ceases to be obligated to perform the functions, activities, and services described in Article III.

C. Upon Covered Entity's knowledge of a material breach or violation of this Agreement by Business Associate, Covered Entity shall notify Business Associate of such breach or violation and Business Associate shall have thirty (30) days to cure the breach or end the violation. In the event Business Associate does not cure the breach or end the violation, Covered Entity shall have the right to immediately terminate this Agreement and any underlying services agreement if feasible.

D. INTENTIONALLY OMITTED.

E. Upon termination of this Agreement, Business Associate will return to Covered Entity, or if return is not feasible, destroy, any and all PHI that it created or received on behalf of Covered Entity and retain no copies thereof. If the return or destruction of the PHI is determined by Business Associate not to be feasible, Business Associate shall limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible. If return or destruction of the PHI is feasible but Business Associate is required by law to retain such information or copies thereof, Business Associate will maintain the PHI for the period of time required under applicable law after which time Business Associate shall return or destroy the PHI.

F. Business Associate's obligations under Sections II and III of this Agreement shall survive the termination of this Agreement with respect to any PHI so long as it remains in the possession of Business Associate.

VI. Other Provisions

A. The parties acknowledge that the foregoing provisions are designed to comply with the mandates of the Privacy and Security Rules and the HITECH Standards and agree to make any necessary changes to this agreement that may be required by any amendment to the final regulations promulgated by the Secretary If the parties are unable to reach agreement regarding an amendment within thirty (30 days) of the date that Business Associate receives any written objection from Covered Entity, either party may terminate this Agreement upon ninety (90) days written notice to the other party. Any other amendment to the Agreement unrelated to compliance with applicable law and regulations shall be effective only upon execution of a written agreement between the parties.

B. Except as it relates to the use, security and disclosure of PHI and electronic transactions, this Agreement is not intended to change the terms and conditions of, or the rights and obligations of the parties under any other services agreement between them.

C. Business Associate agrees to defend, indemnify and hold harmless Covered Entity, its affiliates and each of their respective directors, officers, employees, agents or assigns from and against any and all actions, causes of action, claims, suits and demands whatsoever, and from all damages, liabilities, costs, charges, debts, fines, government investigations, proceedings, and expenses whatsoever (including reasonable attorneys' fees and expenses related to any litigation or other defense of any claims), which may be asserted or for which they may now or hereafter become subject arising in connection with (i) any misrepresentation, breach of warranty or non-fulfillment of any undertaking on the part of Business Associate under this Agreement; and (ii) any claims, demands, awards, judgments, actions, and proceedings made by any person or organization arising out of or in any way connected with Business Associate's performance under this Agreement.

D. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

E. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits the Covered Entity to comply with the Privacy and Security Rules and the HITECH Standards.

F. If any provision of this Agreement is held illegal, invalid, prohibited or unenforceable by a court of competent jurisdiction, that provision shall be limited or eliminated in that jurisdiction to the minimum extent necessary so that this Agreement shall otherwise remain in full force and effect and enforceable

G. This Agreement replaces and supersedes in its (their) entirety any prior Business Associate Agreement(s) between the parties.

[SIGNATURE PAGE TO FOLLOW]

IN WITNESS WHEREOF, this Agreement has been signed and delivered as of the date first set forth above.

Public Education Employees' Health Insurance Board, the Plan Sponsor, acting on behalf of Covered Entity	**<Business Associate>**
_____	_____
Signature	*Signature*
_____	_____
Printed Name	*Printed Name*
_____	_____
Title	*Title*

PEEHIP STATEMENT ON HIPAA COMPLIANCE DOCUMENTATION

The Public Education Employees' Health Insurance Plan (the "Plan") considers personal information to be confidential. The Plan protects the privacy of personal information in accordance with applicable privacy laws. The Plan is required by law to take reasonable steps to ensure the privacy of our members' healthcare information in accordance with the Health Information Portability and Accountability Act (HIPAA). With the recent addition of the Health Information Technology for Economic and Clinical Health (**HITECH**) Act, (enacted as part of the American Recovery and Reinvestment Act of 2009) it is imperative that PEEHIP maintain reasonable oversight over protected health information that it shares with its business associates. As defined by HIPAA, a business associate is any organization or person working in association with, or providing services to, a covered entity (PEEHIP) who handles or discloses Personal Health Information (PHI) or Personal Health Records (PHR).

Proposed Policy:

PEEHIP shall ensure that all of its business associate agreements (BAA's) meet current regulation requirements and are reviewed annually. Any addendum(s) to a BAA that are required by any current or proposed HIPAA or HITECH statutes or regulations shall be entered into within the time frame mandated pursuant to such statutes or regulations.

As a continued or future business associate of PEEHIP, business associates must provide adequate documentation stating they are in compliance with current HIPAA Security and Privacy rules. Documentation must consist of, at a minimum, one of the following:

- **External HIPAA Audit Certification** – Audit must have been conducted by a credible third party audit firm specializing in HIPAA audits within the last two years or within the last 12 months of a significant change or enacted legislation. Summary must state if business associate meets HIPAA compliance.

- **Detailed Internal Controls Documentation** – Policy and audit documentation demonstrating full compliance with each of the standards outlined in the HIPAA Security and Privacy regulations to be reviewed and approved by RSA's security and privacy officials. The HIPAA Privacy and Security Rules are defined in 45 CFR 164 Subparts A and C for Security and Privacy. The HIPAA Security Rule Implementation Standards are outlined in 45 CFR 164.308 - 164.316.

- **Statement of Controls Audit -** At minimum a SOC 1 report is required but a SOC 2 Type 2 certification is preferred as it evolves to become the standard certification for validating confidentiality, availability, and processing integrity within an organization.

  The SOC 2 audit is a replacement for SAS70 Type II. A *SSAE 16 SOC 1* generally covers the financial side of the controls audit; therefore, PEEHIP prefers a SOC 2. Audit documentation must depict controls over systems, operations, and facilities where "PEEHIP" data will be processed and stored for the duration of the contract. *A SOC 3 Report is considered acceptable documentation as it can be freely distributed (general use) and only reported on if the entity has achieved the Trust Services criteria* ***based upon the SOC 2 audit****.*

If a current business associate fails to comply with this Policy, PEEHIP shall have the right, at PEEHIP's sole discretion, to request one of the above defined audits to be completed and results obtained **within 90 days from the date such business associate receives written notice of noncompliance from PEEHIP. In such event, the audited party will be solely responsible for all expenses incurred by the parties during the audit, including without limitation, all payment due to the audit firm. Should such business associate not obtain the audit within the 90 days allowed, PEEHIP shall have the right, in its sole discretion, to terminate its relationship with the business associate. In no event shall a new business associate relationship be created with a party not in compliance with this policy.**

Third Party Vendor – Security Questionnaire

Proposer Name: **Date:**

Prepared By: **Title:**

Factors:

	I. Security Policy	YES/NO/NA	Comments
	A. Policy		
1	Is there a corporate information security policy in place? If yes, provide as an attachment.		
2	Does the policy state what is and is not permissible as it pertains to sensitive company and customer information?		
3	Does the policy identify what is classified as sensitive company and customer information?		
4	Does the policy identify management and employee responsibilities including contractors?		
5	Does the policy identify use of employee owned devices such as laptops, smart phones, and any other form of device capable of storing data?		
6	Does the policy address change management requirements?		
7	Is there a policy on the portable media?(e.g., thumb drives, CDRW, etc.)		
8	Are personnel and contract personnel required to have national background check performed as part of your security policy? Please provide a copy of Proposers personnel policy if this is separate addressing hiring and termination procedures.		
	B. Procedures		
1	Are procedures in place to implement the information security policy?		
2	Are the procedures and standards evaluated to determine their level of impact to the business process?		
3	Does the project management methodology uphold the security practices? If yes, explain how.		
4	Are there policy and procedures in place to vet and audit subcontractors prior to contract acceptance where applicable?		
	C. Document Handling		
1	Is there a reasonable and usable information classification policy?		
2	Does the information classification policy address all enterprise information?		
3	Is an information classification methodology in place to assist employees in identifying levels of information within the business unit?		

4	Is there an information handling matrix that explains how specific information resources are to be handled?
	II. Corporate Practices
	A. Organizational Suitability
1	The Information Security Program has an executive level committee assigned for reporting and guidance purposes?
2	Are employees able to perform their duties efficiently and effectively while following security procedures?
3	Does the information security program have its' own line item in the budget?
4	Does the security group have the authority to submit needed security policy changes throughout the enterprise?
5	Is an annual report on the level of information security compliance issued to management?
6	Is there more than one person responsible for the implementation of the Information Security Program?
	B. Personnel Issues
1	Are employees able to work less than a 50 hour work week on a monthly average and complete their assignments?
2	Are employees and project managers aware of their responsibilities for protecting information resources via written policy?
3	Are technical employees formally trained to perform their tasks?
4	Are contract personnel subject to confidentiality agreements?
5	Are contract personnel subject to the same policies employees are?
6	Is access to sensitive/confidential information by contract personnel monitored?
7	Are national background checks performed on all proposing party employees?
8	Is a similar screening process carried out for contractors and temporary staff?
9	Does employment application ask if the prospective employee has ever been convicted of a crime? If so, does proposing firm employee individuals with felony convictions?
10	Are prior employment verifications performed for initial employment?
11	Are there any current or pending litigations against staff, former staff, or contract staff regarding corporate espionage, identity theft, or any other areas regarding the security of privacy of confidential information?
	C. Training and Education
1	Do employees receive security related training specific to their responsibilities? If yes, please attach a sample.

2	Are employees receiving both positive and negative feedback related to security on their performance evaluations?
3	Is security-related training provided periodically to reflect changes and new methods?
4	Are system administrators given additional security training specific to their jobs?
5	Have employees undergone a HIPAA training class for those handling personal health information (PHI)?
	D. Oversight and Auditing
1	Is Proposer at minimum AICPA SOC 1 Type 2 compliant for financial reporting. If so, please provide the SOC report(s).
2	Is Proposer's datacenter AICPA SOC 2 Type 2 compliant? If not please comment what compliance level your datacenter facility meets.
3	Are the security policies and procedures routinely tested?
4	Are exceptions to security policies and procedures justified and documented?
5	Are audit logs or other reporting mechanisms in place on all platforms?
6	Are errors and failures tracked?
7	When an employee is found to in non-compliance with security policies, has appropriate disciplinary action been taken?
8	Are audits performed on an annual basis?
9	Are unscheduled/surprise audits performed?
10	Has someone been identified as responsible for reconciling audits?
11	Does either an internal or external auditor independently audit Proposer's operational controls on a periodic basis?
12	Is an independent review carried out in order to assess the effective implementation of security policies?
13	Can the Proposer provide evidence of having gone through a recent audit of their organization's operational policies, procedures, and operating effectiveness, such as a SOC Type 2 report?
14	Have audits been performed focusing on HIPAA, PCI, or SOX compliance? If so please, provide a copy.
15	Has Proposer experienced a security breach of corporate or customer data within the last 10 years?
16	Is there is any concluded or pending litigation against the Proposer or an employee related to a contract engagement or security breach?
17	Is Proposers software solution or where data is stored compliant with HIPAA requirements?
18	Does Proposer have a change management committee? Does it meet on regularly scheduled intervals?

	E. Application Development and Management
1	Has an application development methodology been implemented?
2	Are appropriate/key application users involved with developing and improving application methodology and implementation process?
3	Is pre-production testing performed in an isolated environment?
4	Has a promotion to production procedures been implemented?
5	Is there a legacy application management program?
6	Are secure coding standards implemented and are they followed?
7	Are applications testing for security vulnerabilities prior to being released to production?
8	Is there a dedicated security team for testing applications for vulnerabilities?
9	Are there procedures in place for protecting source code developed by the Proposer (physically and electronically)?
10	Is system access and security based on the concept of least possible privilege and need-to-know?
11	Does Proposer perform source code reviews for each release?
12	Are backdoors prevented from being placed into application source code?
	III Physical Security
	A. Physical and Facilities
1	Is access to the building(s) controlled?
2	Is access to computing facilities controlled more so than to the building?
3	Is there an additional level of control for after-hours access?
4	Is there an audit log to identify the individual and the time of access that is monitored by a group other than Information Technology?
5	Are systems and other hardware adequately protected from theft?
6	Are procedures in place for proper disposal of confidential information?
7	Are proper fire suppression systems located in the facility?
8	Are facilities more than 5 miles from a government facility or airport?
9	Are the servers and facilities that house software documentation and programming logic located in a secure facility?
10	Is all confidential and restricted information marked as such and stored in a secure area (room, cabinet) with access restricted to authorized personnel only?
11	Does Proposer allow employees to work remote or in a virtual environment? Please provide documentation around controls for safeguarding computer systems and confidential data.
	B. After-Hours Review
1	Are areas containing sensitive information properly secured?
2	Are workstations secured after-hours?
3	Are keys and access cards properly secured?

4	Is confidential information properly secured?
5	Are contract cleaning crews activities monitored?
	C. Incident Handling
1	Has an Incident Response Team (IRT) been established?
2	Have employees been trained as to when the IRT should be notified?
3	Has the IRT been trained in evidence gathering and handling?
4	Are incident reports issued to appropriate management?
5	After an incident, are policies and procedures reviewed to determine if modification need to be implemented?
6	Does the Proposer have a process in place to notify IT security of breaches and/or problems so that proper notification and correction can be done?
	D. Contingency Planning
1	Has a Business Impact Analysis been conducted on all systems, applications, and platforms?
2	Is there a documented data center Disaster Recovery Plan (DRP) in place?
3	Are backup media password protected or encrypted?
4	Has the data center DRP been tested within the past 12 months?
5	Are system, application, and data backups sent to a secure off-site facility on a regular basis?
6	Are Service Level Agreements that identify processing requirements in place with all users and service providers?
7	Have departments, business units, groups, and other such entities implemented business continuity plans that supplement the data center DRP?
8	Have Emergency Response Procedures (ERP) been implemented?
9	Have ERPs been tested for effectiveness?
	IV. Business Impact Analysis, Disaster Recovery Plan **A. General Review**
1	Backup planning includes identification of all critical data, programs, documentation, and support items required performing essential task during recovery?
2	The BIA is reviewed and updated regularly with special attention to new technology, business changes, and migration of applications to alternative platforms?
3	Critical period timeframes have been identified for all applications and systems?
4	Senior management has reviewed and approved the prioritized list of critical applications?
	B. Disaster Recovery Plan (DRP)

1	A corporate Disaster recovery plan coordinator has been named and a mission statement identifying scope and responsibilities has been published?
2	A "worst-case" scenario DRP to recover normal operations within the prescribed timeframes has been implemented and tested?
3	Listing of current emergency telephone numbers for police, fire department, medical aid, and company officials are strategically located throughout the facility and at off-site locations?
4	The backup site is remote from hazards that endanger the main data center?
5	Contracts for outsourced activities have been amended to include service providers' responsibilities for DRP?
6	Lead times for communication lines and equipment, specialized devices, power hookups, construction, firewalls, computer configurations, and LAN implementation have been factored into the DRP?
7	At least one copy of the DRP is stored at the backup site and is updated regularly?
8	Automatic restart and recovery procedures are in place to restore data files in the event of a processing failure?
9	Contingency arrangements are in place for hardware, software, communications, software, staff and supplies.
10	Customer software solutions that are being developed and\or in production are backed up as part of the Proposer's backup and recovery procedures?
	C. Testing
1	Backup and recovery procedures are tested at least annually?
2	Training sessions are conducted for all relevant personnel on backup, recovery, and contingency operating procedures?
3	Appropriate user representative have a particular role in creating and reviewing control reliability and backup provisions for relevant applications?
4	Appropriate user representatives participate in the DRP tests?
	Other Issues
1	Provisions are in place to maintain the security of processing functions in the event of an emergency?
2	Insurance coverage for loss of hardware and business impact is in place?
	V. Technical Safeguards
	A. Passwords
1	Are host systems and servers as well as application servers secured with unique passwords?
2	Are default accounts de-activated?
3	Are temporary user accounts restricted and disabled within 4 hours?

4	Are the password management systems forcing users to change passwords every 90 days or less?
5	Are users of all company-provided network resources required to change the initial default password?
6	Are the passwords complex? Contain upper case, lower case, special character or number, and at least 8 characters long.
7	Do network and system administrators have adequate experience to implement security standards?
8	Are reports and logs pertaining to network users reviewed and reconciled on a regular basis?
9	Are permissions being set securely?
10	Are administrators assigned a unique ID for access to critical systems?
11	Are administrators using appropriate tools to perform their jobs?
12	Does the application support multi-factor authentication?
13	Are online systems always secured using SSL encryption?
	B. Infrastructure
1	Is the network infrastructure audited on an annual basis?
2	Are network vulnerability assessments conducted on an annual basis?
3	Are changes/improvements made in a timely fashion following network vulnerability assessments?
4	If you house or develop solutions around credit card transactions are you CISP compliant?
	C. Firewalls
1	Are protocols allowed to initiate connections from "outside" the firewall?
2	Has a risk analysis been conducted to determine if the protocols allowed maintain an acceptable level of risk?
3	Has the firewall been tested to determine if outside penetration is possible?
4	Are other products in place to augment the firewall level security?
5	Are the firewalls maintained and monitored 24x7?
6	Have services offered across the firewall been documented?
7	Has a Demilitarized Zone (DMZ) or Perimeter Network been implemented?
8	Has the firewall administrator been formally trained?
9	Is there more than one person administering the firewall?
10	Is the firewall for the ASP separate from the corporate firewall?
	D. Data Communications
1	Is there a remote access procedure in place?
2	Is there a current network diagram?
3	Are Access Control List (ACLs) maintained on a regular basis?
4	Is the network environment partitioned?
5	Are the corporate routers separated from the ASP routers?

6	Are the corporate switches separated from the ASP switches?
7	Does the communication equipment log administrative access to the systems?
8	Is SNMP data collected from the data communication devices?
9	Is syslog data collected from the data communication devices?
10	Are there standard templates for configuring routers?
11	Are there standard templates for configuring switches?
	E. Databases
1	Are default database passwords changed?
2	Are database administrators trained or certified?
3	Are database backups performed daily?
	F. Computing Platforms
1	Are critical servers protected with appropriate access controls?
2	Are development staff administrators on their computers used for writing source code?
3	Is there a company image used for corporate PCs and laptops?
4	Does the company have an asset management system to track software installed?
5	Is there an anti-virus application installed on all PC's, laptops, and servers?
6	Does the anti-virus application automatically update computing assets 3 times or more per day?
7	Is there a URL filtering solution in place?
8	Do computing assets have a corporate anti-malware application installed?
9	Are Internet facing servers protected with host based intrusion prevention?
10	Are employees restricted to what can be installed on their computer systems? How is this managed for remote employees if applicable?
11	Do any of the Proposer's computer systems including storage reside on a cloud computing environment? Is it owned and operated by the Proposer? If no, please explain.
	G. Intrusion Prevention
1	Is host based intrusion prevention software installed on all Internet facing servers?
2	Are network based intrusion prevention systems in-line and defending?
3	Is host based intrusion prevention software installed on all laptops?
4	Is there a dedicated security staff monitoring 24x7 alerts from the host based intrusion prevention?
5	Is there a dedicated security staff monitoring 24x7 alerts from the network based intrusion prevention?
	VI. Telecommunications Security
	A. Policy

1	Is there a published policy on the use of organizational telecommunications resources?
2	Have all employees have been made aware of the telecommunications policy?
3	Employees authorized for Internet access are made aware of the organization's proprietary information and what they can discuss in open forums?
4	Employees using cellular or wireless phones are briefed on the lack of privacy of conversations when using unsecured versions of technology?
5	The organization has a published policy on prosecution of employees and outsiders if found guilty of serious premeditated criminal acts against the organization?
6	Are corporate devices such as iPhones or Android based phones centrally managed by the Proposer to control rogue software installations and protect corporate data?
	B. Standards
1	A threshold is established to monitor and suspend repeated unsuccessful dial-in or remote access attempts?
2	Access to databases reachable via dial-in or VPN have access control in place to prevent unauthorized access?
3	Financial applications available via dial-in or VPN have audit trails established to track access and transaction usage?
4	Are audit trails reviewed and corrective action taken on a regular basis?
5	When possible are acl security programs used to control dial-in or remote access to a specific application?
6	Company proprietary data, stored on portable computers are secured from unauthorized access?
7	Are corporate emails allowed to be sent from unique domains not one used by Proposer such as Gmail or Microsoft Email?
8	Users of all company-provided communication systems are required to change the default or initial password?
	C. Practices
1	Security, application, and network personnel actively work to ensure control inconvenience is as minimal as possible?
2	Personnel independent of the operations staff and security administration review tamper-resistant logs and audit trails?
3	Special procedures and audited user IDs have been established for application, system, network troubleshooting activities?
4	Messages and transactions coming in via phone lines are serially numbered, time stamped, and logged for audit investigation and backup purposes?
5	Employees are made aware of their responsibility to keep remote access codes secure from unauthorized access and usage?

6	Removal of portable computers from the corporate locations must be done through normal property removal procedures?
7	Employees are briefed on their responsibility to protect the property of the company when working away from the corporate environment?

VII. Company Information

	A. Public Information
1	Is the company publicly traded?
2	Is the company bonded?
3	Are all employees in the continental US? If not please list.
	B. Private Information
1	Are there any planned acquisitions in the next 12 months?
2	Are there current plans to sell the company in the next 12 months?

Form **W-9**
(Rev. December 2011)
Department of the Treasury
Internal Revenue Service

Request for Taxpayer Identification Number and Certification

Give Form to the requester. Do not send to the IRS.

Print or type
See **Specific Instructions** on page 2.

Name (as shown on your income tax return)

Business name/disregarded entity name, if different from above

Check appropriate box for federal tax classification:

☐ Individual/sole proprietor ☐ C Corporation ☐ S Corporation ☐ Partnership ☐ Trust/estate

☐ Limited liability company. Enter the tax classification (C=C corporation, S=S corporation, P=partnership) ▸

☐ Other (see instructions) ▸

☐ Exempt payee

Address (number, street, and apt. or suite no.)

Requester's name and address (optional)

City, state, and ZIP code

List account number(s) here (optional)

Part I Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. The TIN provided must match the name given on the "Name" line to avoid backup withholding. For individuals, this is your social security number (SSN). However, for a resident alien, sole proprietor, or disregarded entity, see the Part I instructions on page 3. For other entities, it is your employer identification number (EIN). If you do not have a number, see *How to get a TIN* on page 3.

Note. If the account is in more than one name, see the chart on page 4 for guidelines on whose number to enter.

Social security number

			–			–			

Employer identification number

		–							

Part II Certification

Under penalties of perjury, I certify that:

1. The number shown on this form is my correct taxpayer identification number (or I am waiting for a number to be issued to me), and
2. I am not subject to backup withholding because: (a) I am exempt from backup withholding, or (b) I have not been notified by the Internal Revenue Service (IRS) that I am subject to backup withholding as a result of a failure to report all interest or dividends, or (c) the IRS has notified me that I am no longer subject to backup withholding, and
3. I am a U.S. citizen or other U.S. person (defined below).

Certification instructions. You must cross out item 2 above if you have been notified by the IRS that you are currently subject to backup withholding because you have failed to report all interest and dividends on your tax return. For real estate transactions, item 2 does not apply. For mortgage interest paid, acquisition or abandonment of secured property, cancellation of debt, contributions to an individual retirement arrangement (IRA), and generally, payments other than interest and dividends, you are not required to sign the certification, but you must provide your correct TIN. See the instructions on page 4.

Sign Here **Signature of U.S. person** ▸ **Date** ▸

General Instructions

Section references are to the Internal Revenue Code unless otherwise noted.

Purpose of Form

A person who is required to file an information return with the IRS must obtain your correct taxpayer identification number (TIN) to report, for example, income paid to you, real estate transactions, mortgage interest you paid, acquisition or abandonment of secured property, cancellation of debt, or contributions you made to an IRA.

Use Form W-9 only if you are a U.S. person (including a resident alien), to provide your correct TIN to the person requesting it (the requester) and, when applicable, to:

1. Certify that the TIN you are giving is correct (or you are waiting for a number to be issued),
2. Certify that you are not subject to backup withholding, or
3. Claim exemption from backup withholding if you are a U.S. exempt payee. If applicable, you are also certifying that as a U.S. person, your allocable share of any partnership income from a U.S. trade or business is not subject to the withholding tax on foreign partners' share of effectively connected income.

Note. If a requester gives you a form other than Form W-9 to request your TIN, you must use the requester's form if it is substantially similar to this Form W-9.

Definition of a U.S. person. For federal tax purposes, you are considered a U.S. person if you are:

- An individual who is a U.S. citizen or U.S. resident alien,
- A partnership, corporation, company, or association created or organized in the United States or under the laws of the United States,
- An estate (other than a foreign estate), or
- A domestic trust (as defined in Regulations section 301.7701-7).

Special rules for partnerships. Partnerships that conduct a trade or business in the United States are generally required to pay a withholding tax on any foreign partners' share of income from such business. Further, in certain cases where a Form W-9 has not been received, a partnership is required to presume that a partner is a foreign person, and pay the withholding tax. Therefore, if you are a U.S. person that is a partner in a partnership conducting a trade or business in the United States, provide Form W-9 to the partnership to establish your U.S. status and avoid withholding on your share of partnership income.

The person who gives Form W-9 to the partnership for purposes of establishing its U.S. status and avoiding withholding on its allocable share of net income from the partnership conducting a trade or business in the United States is in the following cases:

- The U.S. owner of a disregarded entity and not the entity,
- The U.S. grantor or other owner of a grantor trust and not the trust, and
- The U.S. trust (other than a grantor trust) and not the beneficiaries of the trust.

Foreign person. If you are a foreign person, do not use Form W-9. Instead, use the appropriate Form W-8 (see Publication 515, Withholding of Tax on Nonresident Aliens and Foreign Entities).

Nonresident alien who becomes a resident alien. Generally, only a nonresident alien individual may use the terms of a tax treaty to reduce or eliminate U.S. tax on certain types of income. However, most tax treaties contain a provision known as a "saving clause." Exceptions specified in the saving clause may permit an exemption from tax to continue for certain types of income even after the payee has otherwise become a U.S. resident alien for tax purposes.

If you are a U.S. resident alien who is relying on an exception contained in the saving clause of a tax treaty to claim an exemption from U.S. tax on certain types of income, you must attach a statement to Form W-9 that specifies the following five items:

1. The treaty country. Generally, this must be the same treaty under which you claimed exemption from tax as a nonresident alien.

2. The treaty article addressing the income.

3. The article number (or location) in the tax treaty that contains the saving clause and its exceptions.

4. The type and amount of income that qualifies for the exemption from tax.

5. Sufficient facts to justify the exemption from tax under the terms of the treaty article.

Example. Article 20 of the U.S.-China income tax treaty allows an exemption from tax for scholarship income received by a Chinese student temporarily present in the United States. Under U.S. law, this student will become a resident alien for tax purposes if his or her stay in the United States exceeds 5 calendar years. However, paragraph 2 of the first Protocol to the U.S.-China treaty (dated April 30, 1984) allows the provisions of Article 20 to continue to apply even after the Chinese student becomes a resident alien of the United States. A Chinese student who qualifies for this exception (under paragraph 2 of the first protocol) and is relying on this exception to claim an exemption from tax on his or her scholarship or fellowship income would attach to Form W-9 a statement that includes the information described above to support that exemption.

If you are a nonresident alien or a foreign entity not subject to backup withholding, give the requester the appropriate completed Form W-8.

What is backup withholding? Persons making certain payments to you must under certain conditions withhold and pay to the IRS a percentage of such payments. This is called "backup withholding." Payments that may be subject to backup withholding include interest, tax-exempt interest, dividends, broker and barter exchange transactions, rents, royalties, nonemployee pay, and certain payments from fishing boat operators. Real estate transactions are not subject to backup withholding.

You will not be subject to backup withholding on payments you receive if you give the requester your correct TIN, make the proper certifications, and report all your taxable interest and dividends on your tax return.

Payments you receive will be subject to backup withholding if:

1. You do not furnish your TIN to the requester,

2. You do not certify your TIN when required (see the Part II instructions on page 3 for details),

3. The IRS tells the requester that you furnished an incorrect TIN,

4. The IRS tells you that you are subject to backup withholding because you did not report all your interest and dividends on your tax return (for reportable interest and dividends only), or

5. You do not certify to the requester that you are not subject to backup withholding under 4 above (for reportable interest and dividend accounts opened after 1983 only).

Certain payees and payments are exempt from backup withholding. See the instructions below and the separate Instructions for the Requester of Form W-9.

Also see *Special rules for partnerships* on page 1.

Updating Your Information

You must provide updated information to any person to whom you claimed to be an exempt payee if you are no longer an exempt payee and anticipate receiving reportable payments in the future from this person. For example, you may need to provide updated information if you are a C corporation that elects to be an S corporation, or if you no longer are tax exempt. In addition, you must furnish a new Form W-9 if the name or TIN changes for the account, for example, if the grantor of a grantor trust dies.

Penalties

Failure to furnish TIN. If you fail to furnish your correct TIN to a requester, you are subject to a penalty of $50 for each such failure unless your failure is due to reasonable cause and not to willful neglect.

Civil penalty for false information with respect to withholding. If you make a false statement with no reasonable basis that results in no backup withholding, you are subject to a $500 penalty.

Criminal penalty for falsifying information. Willfully falsifying certifications or affirmations may subject you to criminal penalties including fines and/or imprisonment.

Misuse of TINs. If the requester discloses or uses TINs in violation of federal law, the requester may be subject to civil and criminal penalties.

Specific Instructions

Name

If you are an individual, you must generally enter the name shown on your income tax return. However, if you have changed your last name, for instance, due to marriage without informing the Social Security Administration of the name change, enter your first name, the last name shown on your social security card, and your new last name.

If the account is in joint names, list first, and then circle, the name of the person or entity whose number you entered in Part I of the form.

Sole proprietor. Enter your individual name as shown on your income tax return on the "Name" line. You may enter your business, trade, or "doing business as (DBA)" name on the "Business name/disregarded entity name" line.

Partnership, C Corporation, or S Corporation. Enter the entity's name on the "Name" line and any business, trade, or "doing business as (DBA) name" on the "Business name/disregarded entity name" line.

Disregarded entity. Enter the owner's name on the "Name" line. The name of the entity entered on the "Name" line should never be a disregarded entity. The name on the "Name" line must be the name shown on the income tax return on which the income will be reported. For example, if a foreign LLC that is treated as a disregarded entity for U.S. federal tax purposes has a domestic owner, the domestic owner's name is required to be provided on the "Name" line. If the direct owner of the entity is also a disregarded entity, enter the first owner that is not disregarded for federal tax purposes. Enter the disregarded entity's name on the "Business name/disregarded entity name" line. If the owner of the disregarded entity is a foreign person, you must complete an appropriate Form W-8.

Note. Check the appropriate box for the federal tax classification of the person whose name is entered on the "Name" line (Individual/sole proprietor, Partnership, C Corporation, S Corporation, Trust/estate).

Limited Liability Company (LLC). If the person identified on the "Name" line is an LLC, check the "Limited liability company" box only and enter the appropriate code for the tax classification in the space provided. If you are an LLC that is treated as a partnership for federal tax purposes, enter "P" for partnership. If you are an LLC that has filed a Form 8832 or a Form 2553 to be taxed as a corporation, enter "C" for C corporation or "S" for S corporation. If you are an LLC that is disregarded as an entity separate from its owner under Regulation section 301.7701-3 (except for employment and excise tax), do not check the LLC box unless the owner of the LLC (required to be identified on the "Name" line) is another LLC that is not disregarded for federal tax purposes. If the LLC is disregarded as an entity separate from its owner, enter the appropriate tax classification of the owner identified on the "Name" line.

Other entities. Enter your business name as shown on required federal tax documents on the "Name" line. This name should match the name shown on the charter or other legal document creating the entity. You may enter any business, trade, or DBA name on the "Business name/ disregarded entity name" line.

Exempt Payee

If you are exempt from backup withholding, enter your name as described above and check the appropriate box for your status, then check the "Exempt payee" box in the line following the "Business name/ disregarded entity name," sign and date the form.

Generally, individuals (including sole proprietors) are not exempt from backup withholding. Corporations are exempt from backup withholding for certain payments, such as interest and dividends.

Note. If you are exempt from backup withholding, you should still complete this form to avoid possible erroneous backup withholding.

The following payees are exempt from backup withholding:

1. An organization exempt from tax under section 501(a), any IRA, or a custodial account under section 403(b)(7) if the account satisfies the requirements of section 401(f)(2),

2. The United States or any of its agencies or instrumentalities,

3. A state, the District of Columbia, a possession of the United States, or any of their political subdivisions or instrumentalities,

4. A foreign government or any of its political subdivisions, agencies, or instrumentalities, or

5. An international organization or any of its agencies or instrumentalities.

Other payees that may be exempt from backup withholding include:

6. A corporation,

7. A foreign central bank of issue,

8. A dealer in securities or commodities required to register in the United States, the District of Columbia, or a possession of the United States,

9. A futures commission merchant registered with the Commodity Futures Trading Commission,

10. A real estate investment trust,

11. An entity registered at all times during the tax year under the Investment Company Act of 1940,

12. A common trust fund operated by a bank under section 584(a),

13. A financial institution,

14. A middleman known in the investment community as a nominee or custodian, or

15. A trust exempt from tax under section 664 or described in section 4947.

The following chart shows types of payments that may be exempt from backup withholding. The chart applies to the exempt payees listed above, 1 through 15.

IF the payment is for . . .	THEN the payment is exempt for . . .
Interest and dividend payments	All exempt payees except for 9
Broker transactions	Exempt payees 1 through 5 and 7 through 13. Also, C corporations.
Barter exchange transactions and patronage dividends	Exempt payees 1 through 5
Payments over $600 required to be reported and direct sales over $5,000 [1]	Generally, exempt payees 1 through 7 [2]

[1] See Form 1099-MISC, Miscellaneous Income, and its instructions.

[2] However, the following payments made to a corporation and reportable on Form 1099-MISC are not exempt from backup withholding: medical and health care payments, attorneys' fees, gross proceeds paid to an attorney, and payments for services paid by a federal executive agency.

Part I. Taxpayer Identification Number (TIN)

Enter your TIN in the appropriate box. If you are a resident alien and you do not have and are not eligible to get an SSN, your TIN is your IRS individual taxpayer identification number (ITIN). Enter it in the social security number box. If you do not have an ITIN, see *How to get a TIN* below.

If you are a sole proprietor and you have an EIN, you may enter either your SSN or EIN. However, the IRS prefers that you use your SSN.

If you are a single-member LLC that is disregarded as an entity separate from its owner (see *Limited Liability Company (LLC)* on page 2), enter the owner's SSN (or EIN, if the owner has one). Do not enter the disregarded entity's EIN. If the LLC is classified as a corporation or partnership, enter the entity's EIN.

Note. See the chart on page 4 for further clarification of name and TIN combinations.

How to get a TIN. If you do not have a TIN, apply for one immediately. To apply for an SSN, get Form SS-5, Application for a Social Security Card, from your local Social Security Administration office or get this form online at *www.ssa.gov*. You may also get this form by calling 1-800-772-1213. Use Form W-7, Application for IRS Individual Taxpayer Identification Number, to apply for an ITIN, or Form SS-4, Application for Employer Identification Number, to apply for an EIN. You can apply for an EIN online by accessing the IRS website at *www.irs.gov/businesses* and clicking on Employer Identification Number (EIN) under Starting a Business. You can get Forms W-7 and SS-4 from the IRS by visiting IRS.gov or by calling 1-800-TAX-FORM (1-800-829-3676).

If you are asked to complete Form W-9 but do not have a TIN, write "Applied For" in the space for the TIN, sign and date the form, and give it to the requester. For interest and dividend payments, and certain payments made with respect to readily tradable instruments, generally you will have 60 days to get a TIN and give it to the requester before you are subject to backup withholding on payments. The 60-day rule does not apply to other types of payments. You will be subject to backup withholding on all such payments until you provide your TIN to the requester.

Note. Entering "Applied For" means that you have already applied for a TIN or that you intend to apply for one soon.

Caution: *A disregarded domestic entity that has a foreign owner must use the appropriate Form W-8.*

Part II. Certification

To establish to the withholding agent that you are a U.S. person, or resident alien, sign Form W-9. You may be requested to sign by the withholding agent even if item 1, below, and items 4 and 5 on page 4 indicate otherwise.

For a joint account, only the person whose TIN is shown in Part I should sign (when required). In the case of a disregarded entity, the person identified on the "Name" line must sign. Exempt payees, see *Exempt Payee* on page 3.

Signature requirements. Complete the certification as indicated in items 1 through 3, below, and items 4 and 5 on page 4.

1. Interest, dividend, and barter exchange accounts opened before 1984 and broker accounts considered active during 1983. You must give your correct TIN, but you do not have to sign the certification.

2. Interest, dividend, broker, and barter exchange accounts opened after 1983 and broker accounts considered inactive during 1983. You must sign the certification or backup withholding will apply. If you are subject to backup withholding and you are merely providing your correct TIN to the requester, you must cross out item 2 in the certification before signing the form.

3. Real estate transactions. You must sign the certification. You may cross out item 2 of the certification.

4. Other payments. You must give your correct TIN, but you do not have to sign the certification unless you have been notified that you have previously given an incorrect TIN. "Other payments" include payments made in the course of the requester's trade or business for rents, royalties, goods (other than bills for merchandise), medical and health care services (including payments to corporations), payments to a nonemployee for services, payments to certain fishing boat crew members and fishermen, and gross proceeds paid to attorneys (including payments to corporations).

5. Mortgage interest paid by you, acquisition or abandonment of secured property, cancellation of debt, qualified tuition program payments (under section 529), IRA, Coverdell ESA, Archer MSA or HSA contributions or distributions, and pension distributions. You must give your correct TIN, but you do not have to sign the certification.

What Name and Number To Give the Requester

For this type of account:	Give name and SSN of:
1. Individual	The individual
2. Two or more individuals (joint account)	The actual owner of the account or, if combined funds, the first individual on the account [1]
3. Custodian account of a minor (Uniform Gift to Minors Act)	The minor [2]
4. a. The usual revocable savings trust (grantor is also trustee)	The grantor-trustee [1]
b. So-called trust account that is not a legal or valid trust under state law	The actual owner [1]
5. Sole proprietorship or disregarded entity owned by an individual	The owner [3]
6. Grantor trust filing under Optional Form 1099 Filing Method 1 (see Regulation section 1.671-4(b)(2)(i)(A))	The grantor*
For this type of account:	**Give name and EIN of:**
7. Disregarded entity not owned by an individual	The owner
8. A valid trust, estate, or pension trust	Legal entity [4]
9. Corporation or LLC electing corporate status on Form 8832 or Form 2553	The corporation
10. Association, club, religious, charitable, educational, or other tax-exempt organization	The organization
11. Partnership or multi-member LLC	The partnership
12. A broker or registered nominee	The broker or nominee
13. Account with the Department of Agriculture in the name of a public entity (such as a state or local government, school district, or prison) that receives agricultural program payments	The public entity
14. Grantor trust filing under the Form 1041 Filing Method or the Optional Form 1099 Filing Method 2 (see Regulation section 1.671-4(b)(2)(i)(B))	The trust

[1] List first and circle the name of the person whose number you furnish. If only one person on a joint account has an SSN, that person's number must be furnished.

[2] Circle the minor's name and furnish the minor's SSN.

[3] You must show your individual name and you may also enter your business or "DBA" name on the "Business name/disregarded entity" name line. You may use either your SSN or EIN (if you have one), but the IRS encourages you to use your SSN.

[4] List first and circle the name of the trust, estate, or pension trust. (Do not furnish the TIN of the personal representative or trustee unless the legal entity itself is not designated in the account title.) Also see *Special rules for partnerships* on page 1.

***Note.** Grantor also must provide a Form W-9 to trustee of trust.

Note. If no name is circled when more than one name is listed, the number will be considered to be that of the first name listed.

Secure Your Tax Records from Identity Theft

Identity theft occurs when someone uses your personal information such as your name, social security number (SSN), or other identifying information, without your permission, to commit fraud or other crimes. An identity thief may use your SSN to get a job or may file a tax return using your SSN to receive a refund.

To reduce your risk:

- Protect your SSN,
- Ensure your employer is protecting your SSN, and
- Be careful when choosing a tax preparer.

If your tax records are affected by identity theft and you receive a notice from the IRS, respond right away to the name and phone number printed on the IRS notice or letter.

If your tax records are not currently affected by identity theft but you think you are at risk due to a lost or stolen purse or wallet, questionable credit card activity or credit report, contact the IRS Identity Theft Hotline at 1-800-908-4490 or submit Form 14039.

For more information, see Publication 4535, Identity Theft Prevention and Victim Assistance.

Victims of identity theft who are experiencing economic harm or a system problem, or are seeking help in resolving tax problems that have not been resolved through normal channels, may be eligible for Taxpayer Advocate Service (TAS) assistance. You can reach TAS by calling the TAS toll-free case intake line at 1-877-777-4778 or TTY/TDD 1-800-829-4059.

Protect yourself from suspicious emails or phishing schemes. Phishing is the creation and use of email and websites designed to mimic legitimate business emails and websites. The most common act is sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft.

The IRS does not initiate contacts with taxpayers via emails. Also, the IRS does not request personal detailed information through email or ask taxpayers for the PIN numbers, passwords, or similar secret access information for their credit card, bank, or other financial accounts.

If you receive an unsolicited email claiming to be from the IRS, forward this message to *phishing@irs.gov*. You may also report misuse of the IRS name, logo, or other IRS property to the Treasury Inspector General for Tax Administration at 1-800-366-4484. You can forward suspicious emails to the Federal Trade Commission at: *spam@uce.gov* or contact them at *www.ftc.gov/idtheft* or 1-877-IDTHEFT (1-877-438-4338).

Visit IRS.gov to learn more about identity theft and how to reduce your risk.

Privacy Act Notice

Section 6109 of the Internal Revenue Code requires you to provide your correct TIN to persons (including federal agencies) who are required to file information returns with the IRS to report interest, dividends, or certain other income paid to you; mortgage interest you paid; the acquisition or abandonment of secured property; the cancellation of debt; or contributions you made to an IRA, Archer MSA, or HSA. The person collecting this form uses the information on the form to file information returns with the IRS, reporting the above information. Routine uses of this information include giving it to the Department of Justice for civil and criminal litigation and to cities, states, the District of Columbia, and U.S. possessions for use in administering their laws. The information also may be disclosed to other countries under a treaty, to federal and state agencies to enforce civil and criminal laws, or to federal law enforcement and intelligence agencies to combat terrorism. You must provide your TIN whether or not you are required to file a tax return. Under section 3406, payers must generally withhold a percentage of taxable interest, dividend, and certain other payments to a payee who does not give a TIN to the payer. Certain penalties may also apply for providing false or fraudulent information.